JUSTIS Information System for the District of Columbia

Phase 2 Project file

Justice Information System for the District of Columbia

Phase 2 Blueprint Draft

Document History	
Document Filename:	Phase2_Blueprint_Draftver9_14_01
Document Type:	Meeting Notes
Document Status:	Draft
Time of Last Update:	9/14/2001 6:06 PM
Project Name:	DC JUSTIS Phase 2
Contract Number:	DC-C-920-S-065
Document Purpose:	This document details the plan to implement JUSTIS Phase 2.
Revision History	8/31/2000 – JUSTIS POC Blueprint Draft 1/15/2001 – JUSTIS POC Blueprint 6/06/2001 – JUSTIS Phase 2 Blueprint Draft 9/14/2001 – JUSTIS Phase 2 Final Blueprint

~ Table of Contents ~

~ *Figures* ~

1. Introduction

1.1 Background

The Criminal Justice Coordinating Council of the District of Columbia (CJCC) was organized with the following mission:

> To serve as the forum for identifying issues and their solutions, proposing actions, and facilitating cooperation that will improve public safety and the related criminal and juvenile justice services for District of Columbia residents, visitors, victims, and offenders. The CJCC draws upon local and federal agencies and individuals to develop recommendations and strategies for accomplishing this mission. Our guiding principles are creative collaboration, community involvement, and effective resource utilization. We are committed to developing targeted funding strategies and comprehensive management information through integrated information technology systems and social science research in order to achieve our goal.[1]

In 1999, the CJCC of the District of Columbia, supported by its Policy and Budget Working Group (P&BWG), produced a federal funding strategy, recommended a governance structure, and prepared an *Information Technology Interagency Agreement* that the CJCC members adopted. This agreement recognized the need for immediate improvement of information technology in the criminal justice system within the District of Columbia and established the Information Technology Advisory Committee (ITAC) to serve as the governance body for justice system development.

The ITAC has been given the duty of advising and making recommendations to the CJCC in regards to improvement of the information technology infrastructure of justice agencies within the District of Columbia. The recommendations are to be made in respect to increased funding of information technology projects; increased data sharing, access, and integration; improved data and system security, and the development of system-wide standards and measurement of data use and quality, as appropriate to the then-current developmental stage of the justice system. The recommendations by the ITAC are developed based on the following guiding principles:[2]

- Recognize the primacy of each justice agency mission
- Facilitate collaborative solutions to justice information challenges

[1] http://www.cjccdc.org

[2] *Ibid.*

- Commit to the quality and integrity of justice data
- Implement effective data and system security
- Respect the confidentiality of information and individual privacy
- Establishment of system-wide standards, supported by common identifiers and positive identification
- Nurture agency and community requirements for research and public access
- Provide for long-term performance monitoring and evaluation

Early during the formation of the ITAC, the CJCC recognized that the information systems maintained by the justice agencies within the District were difficult to access. The ITAC envisioned a system that would promote the sharing of justice data while maintaining the primacy of each justice agency. The solution is a District of Columbia Justice Information System (JUSTIS).

In July 2000, the CJCC partnered with the Office of the Chief Technology Officer (OCTO) in contracting KPMG Consulting, Inc. to design a solution concept that is based on modern dedicated Intranet and web browser technologies that support secure, confidential data access, data sharing, and notification functionality. It is imperative that the solution concept is designed not to disrupt the existing legacy systems of the individual agencies or demand costly and inefficient data collection and transfer. The design was delivered to the ITAC in the form of a JUSTIS Blueprint. In conjunction with the delivery of the JUSTIS Blueprint, KPMG Consulting, Inc. was also contracted to develop a functioning proof-of-concept (POC). This POC became the initial phase of JUSTIS development and was to serve as a model of data sharing functionality between several CJCC member agencies. Both the JUSTIS Blueprint and the POC were delivered to the ITAC on January 17, 2001.

As a result of the successful demonstration of a data sharing functionality between CJCC member agencies, the CJCC decided to continue the development and implementation of JUSTIS. The CJCC once again partnered with OCTO to contract with KPMG Consulting, Inc. to develop and implement additional data sharing capabilities among member agencies. This extended the development of JUSTIS under the project title, JUSTIS Phase 2. The scheduled delivery date for this phase of JUSTIS is September 18, 2001.

1.2 Implementation Strategy

This document is the Phase 2 Final JUSTIS Blueprint (JUSTIS Blueprint) for the implementation of JUSTIS and is to establish the foundation for the CJCC envisioned solution. The JUSTIS Blueprint is a vision of the ultimate system, an analysis of current state capabilities and requirements, and a definition of steps to take for a

multi-phased implementation. This Blueprint is also to provide a high-level architecture and roadmap for the continued development of JUSTIS.

The JUSTIS Blueprint is developed with the intention of a multi-phased approach. A multi-phased implementation is designed to provide enhanced JUSTIS functionalities to be implemented with phases in a three- to six-month time frame. Such an implementation provides several advantages over a large, full-scale implementation. A phased implementation:

- Provides short-term successes
- Allows time for validation of the long-term plan after each phase
- Allows for the integration of current technologies throughout the implementation

A representative diagram of a possible JUSTIS multi-phased implementation follows:

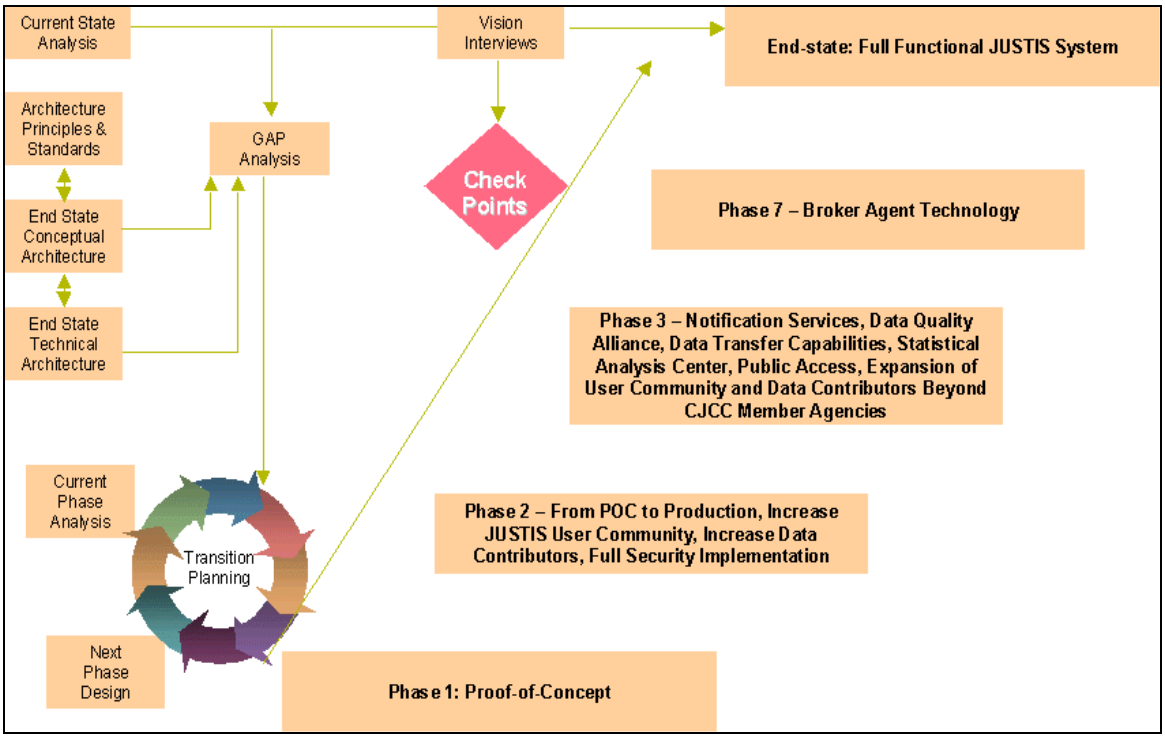


Figure 1 – Representative of JUSTIS Phased Implementation

The beginning of a multi-phase implementation as represented in Figure 1 is an analysis of the current state of the justice agencies' business processes and information technology infrastructure. Coinciding with this analysis is the coordinating

of key justice agency personnel's foresight in the form of "Vision Interviews." System validation points are developed from the vision interviews.

The full functional JUSTIS system is considered "End State" in the figure. The JUSTIS design is derived from a foundation of agreed upon architecture principles and standards. The JUSTIS architecture is refined by the agreed upon principles and standards. The technical architecture of the system is generated from the conceptual architecture. This evolution of the design of JUSTIS creates the End State solution.

Transition planning is the integration of the current state analysis and the end state solution that generates a list of "gap" points. The gap points are logically prioritized according to both business and technological constraints and the aforementioned vision interviews. The prioritization of the gap points develops the multi-phased implementation. Throughout the multi-phased implementation each phase must be validated against the original vision of JUSTIS to ensure the implementation remains true to that vision.

The JUSTIS multi-phased implementation began with the development and deployment of the working proof-of-concept (POC), which was completed in January 2001. The POC used open Internet technologies and standards to link information from diverse justice agency systems as is designed in the complete JUSTIS architecture. The POC gave the CJCC and the selected pilot agencies an early look at the JUSTIS architecture and functionality. Also, selected authorized users were granted access to JUSTIS. This enables users to view the selected shared information and observe and actively participate in the on-going development of JUSTIS.

1.3 Blueprint Format

The Blueprint defines and recommends the necessary elements for the CJCC to continue the implementation of JUSTIS. The Blueprint accomplishes this in the following manner:

1. **Defining the Future JUSTIS User Community and System.** It is important to define the ideal future system first, without concern for the current capabilities. This ensures maximum creativity on the part of the participants. The ITLO provided KPMG Consulting, Inc. with the opportunity for numerous vision interviews with key ITAC members during the months of July and August 2000. We also considered capabilities in the KPMG Consulting, Inc. JNET solution developed for the Commonwealth of Pennsylvania.

2. **Defining the current technical infrastructure in the justice agencies in the District of Columbia.** The first step defined where we want to end up with our JUSTIS. This step describes the point from which we will begin.

3. **Conducting a Gap Analysis.** In this step, we show the distance that needs to be closed in moving from the current state towards the target end state.

4. **Recommendation of the Roadmap that will bring the Future JUSTIS System to reality in the justice agencies within the District of Columbia.** The roadmap recognizes the importance of a phased implementation, as discussed above.

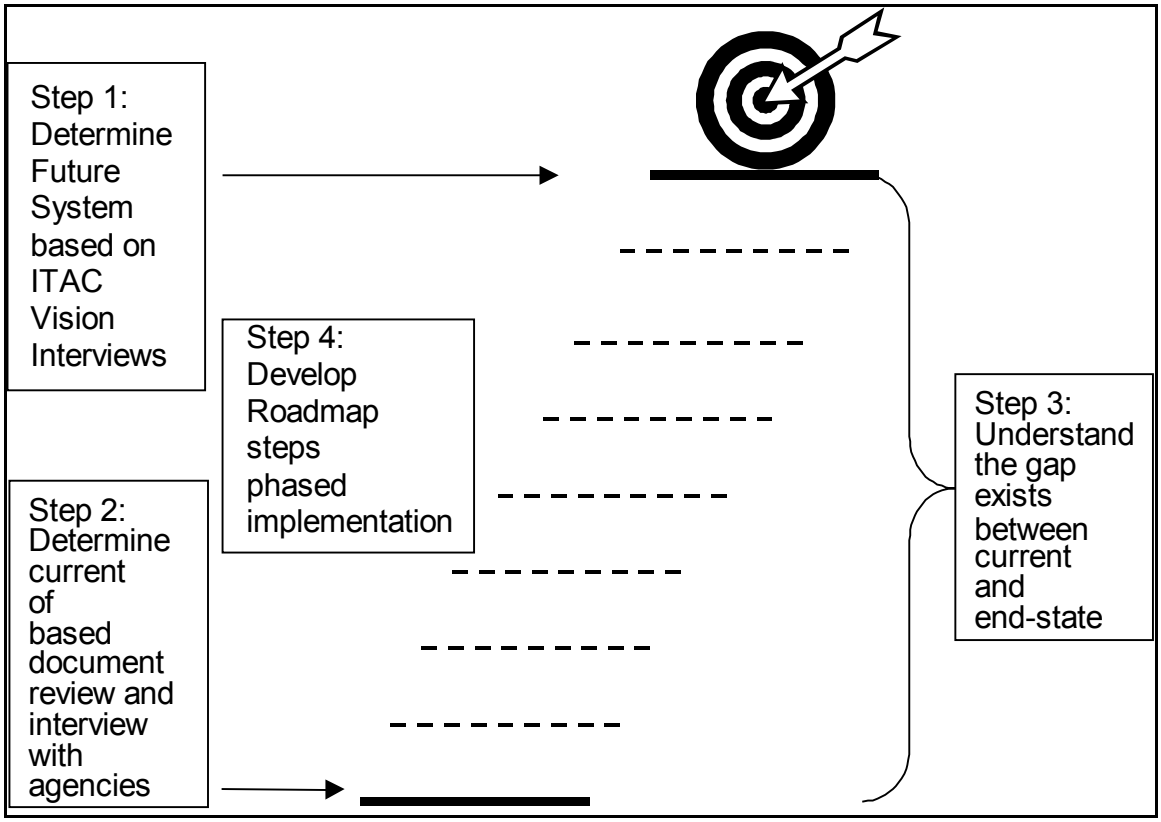


Figure 2 – Blueprint Format

The Blueprint is a "living" document. Therefore, as JUSTIS Phases are developed and implementation paths are followed, it is expected that the Blueprint will be updated in consideration of the following:

- **Initial Phase Definition** – This point is shortly after a Statement of Work (SOW) defined the initial phase. The Blueprint should be updated to include information more specific to the phase as defined in the SOW. The essence of this update is the inclusion of proposed methodologies that will contribute to the success of the phase. This update should also reflect any significant findings gained since the last update.
- **Phase Results** – At this point the implementation team has developed and implemented the functionalities defined by the SOW. The Blueprint is updated to reflect any "lessons learned" during implementation the predefined phase.

- **User Evaluation** – An evaluation period is planned at the end of each phase. At this time the users will be able to express ideas and suggestions about JUSTIS system development. The JUSTIS Blueprint is then updated to include the evaluations and proposed suggestions encompassed in the evaluations.

2. JUSTIS Business Requirements and Goals

2.1 JUSTIS Business Requirements

The CJCC has taken the initiative in pursuing and managing necessary business requirements within the justice community of the District of Columbia that lead to the accomplishment of its stated objectives. These business requirements are continually referenced throughout the development of JUSTIS.

- **Implement industry best practices for information security.** JUSTIS requires system-wide security policies. The CJCC has taken the initiative to develop security policies that meet or exceed the security requirements of the member agencies and draws upon elements from the National Crime Information Center (NCIC) standards.

- **Encourage the use of a common District-wide identifier.** The data shared in JUSTIS can be designed to be retrievable by a common District-wide identifier, such as the PDID. Having a common identifier will enable many of the functions of JUSTIS and will assist justice agencies within the District in coordinating their information processing.

- **Foster interagency participation and collaboration.** JUSTIS enables participation of all District and Federal justice agencies. JUSTIS ease of use creates an environment that promotes interagency participation and collaboration.

- **Streamline processing that cross agency boundaries.** The streamlining of agency processes increases efficiency and effectiveness. The implementation of JUSTIS integrates technology into currently manual process. The reduction of manual processes will streamline processes across agency boundaries.

- **Recognize the independence and primacy of each justice agency**. Although agency coordination and consensus is a necessary business requirement, effective agency governance and representation is just as critical. The development of JUSTIS recognizes agency primacy and is designed to be considerate of individual agency decision-making.

- **Employ open technologies.** The use of open technologies also contributes to the independence of individual agencies. Agencies can make changes to other information systems with minimum impact on JUSTIS.

The CJCC is committed to making the many justice agencies within the District of Columbia function in unison with information sharing as a backbone. The District of Columbia's JUSTIS system is designed to provide a platform for this information sharing through the use of "connections." JUSTIS provides connections between people and information (information inquiry applications and search engines);

connections between people and people (newsgroups, secure email) and connections between information and information (e.g., data transfer, data quality, notification). JUSTIS is designed to contribute to the objectives of the CJCC.

2.2 JUSTIS Goals

In addition to the business requirements imposed on JUSTIS, there are a number of fundamental goals for the system: collaboration, information sharing, effective resource utilization and information management.

2.2.1 Collaboration

Notification applications outlined in JUSTIS provide yet another opportunity for justice agency collaboration. The notification could be on an individual basis or a group basis. For example, when a parolee is arrested and booked, this event (the police booking) can generate a notification to an individual parole officer or group of interested parties.

Another opportunity for collaboration is through the use of discussion groups. Authorized users could participate in on-line discussions regarding justice issues, case management, and the like.

JUSTIS enables collaborative solutions to justice information challenges. Agencies can work together in case management and transition. For example, an offender contact list can be published through JUSTIS. This offender contact list will provide the contact information for case handlers, such as the attorneys assigned to the case, the judge assigned, the arresting law enforcement official, and any other individuals within the justice agencies that could be of importance. The list would provide one area to obtain key contacts for an individual offender.

2.2.2 Information Sharing

Interagency sharing of data supports each agency's ability to make quality decisions. JUSTIS provides a platform for the sharing of critical justice information on a timely basis and in a secure environment. This allows justice agencies to share selected information that will assist each justice agency in conducting its mission-critical activities.

The CJCC decision to take advantage of modern dedicated Intranet and web browser technologies allows for the publishing of data in a timely fashion. One example of an information sharing opportunity that can be enhanced with the implementation of JUSTIS is the accurate identification of court appointed attorneys. Any change in attorney assignment made by the courts can be

"published" (translated to a standard web-accessible format and forwarded) using JUSTIS. Any authorized JUSTIS user could then locate and retrieve the current case disposition of an offender.

2.2.3 *Effective Resource Utilization*

Currently, interagency data exchanges are either not taking place or are performed using inefficient manual processes. JUSTIS allows resources to use information system solutions to become more effective contributors and reduce labor-intensive information searches. For example, many justice agencies are in need of the daily "lock-up list" produced by the Metropolitan Police Department (MPD). The acquisition of this list in a timely manner by each agency requires labor-intensive processes. The implementation of JUSTIS could allow the lock-up list to be published as soon as it is produced by MPD, therefore eliminating any need for other agencies to commit resources in the acquiring of this list.

JUSTIS also allows for the opportunity of data transfer. The concept allows for common data to be identified and captured through the browser. The authorized user could then potentially copy the data and use it to populate a corresponding common data field in the agency's legacy system. This eliminates the redundant activity of re-keying common information from system to system. This also reduces potential errors caused by keying mistakes when transferring data from system to system.

2.2.4 *Information Management*

Information systems for the justice community must implement effective data and system security. JUSTIS provides for indirect data retrieval from agency information systems. This allows for a significant decrease in security risk to the legacy systems and absolutely no risk of data corruption. Authorized users will enter JUSTIS and view published data that has been obtained either through direct access through a firewall to the legacy system, indirect access through a firewall to an intermediary server, or off-line access, where the data is loaded into the JUSTIS agency server through some other media. Thus the inquiry will not have direct unsecured access to the agency legacy system.

Additionally, a tenet of JUSTIS is to not interfere with, compete with, or replace current legacy systems. JUSTIS is not a data warehouse. Therefore there is no central repository of data and the data physically stays within the agency's IT infrastructure unless otherwise requested by the particular agency.

3. Future JUSTIS User Community and System

3.1 Introduction

JUSTIS supports the justice community and each of its member agencies. This section describes the fully functional system, the model that comprises the overall solution, the proposed user community, the technical architecture, and the organizational structure necessary to manage and administer the system.

This section concentrates on describing the future "to be" JUSTIS system. Subsequent sections will address the current state and strategies for getting from where we are to where we want to be. Because this is a Blueprint document, it seems appropriate to use the following building metaphor to organize this section:

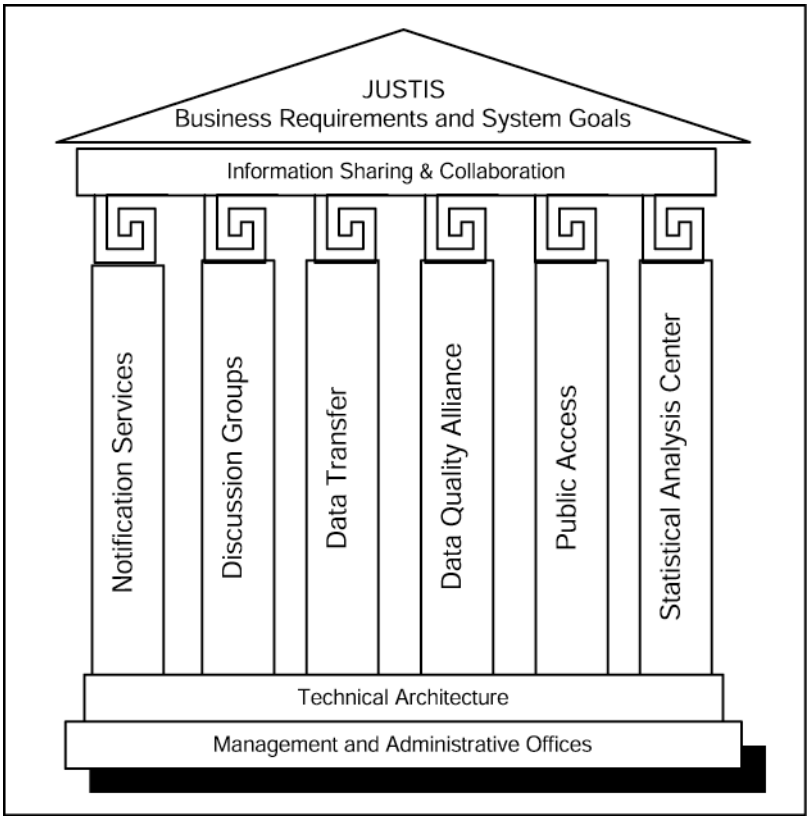


Figure 3 – Blueprint Building Metaphor

In this section, we will start from the top of the diagram and proceed toward the bottom. We have already discussed the business requirements and system goals that JUSTIS is designed to meet. In this section, we will discuss the functional components that empower JUSTIS and its users to achieve the business requirements and system goals. "Information Sharing and Collaboration" is shown

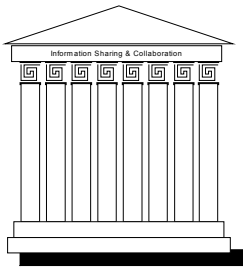
across the top of our diagram because it is the very essence – the capstone – of the system. (See section 3.2 Agency Information Sharing)

We will present the supporting functional components. Shown as columns in the diagram, these functions of JUSTIS support information sharing and collaboration. (See section 3.4 Other Interagency Functions Supported JUSTIS)

We will present the technical architecture that is needed to support the functional components. The functional discussion has shown *what* the system will do. The technical architecture section will show *how* the system will do it. (See section 3.5 Technical Architecture)

Finally, the management and administrative office structure necessary to support JUSTIS is described. Shown at the bottom of our diagram, this organization will be the bedrock and foundation for JUSTIS. (See section 3.6 Management and Administrative Structure)

3.2 Agency Information Sharing and Collaboration



JUSTIS is designed to provide justice agencies a quick and effective way to share justice information and collaborate with colleagues. The value provided by JUSTIS to the user community is in direct relation to the number of participating agencies – both contributors and consumers.

JUSTIS will enable its users to share justice information through a variety of modes:

- **JUSTIS Inquiry Application** – Record queries allow individual JUSTIS agencies to view the public safety data in located in other agencies' systems. The authorized user accesses the inquiry application, enters a query based upon an agency system key, fills the query requirements and submits. The system returns a unified view of queried information. This inquiry can be done contributing agency wide or by individual agency. Note that queries submitted, logins and other user activity are recorded to an audit log.

- **Searches** – Information sharing is improved beyond predetermined queries when information searches are enabled. These searches can be conducted across the entire World Wide Web or within the JUSTIS framework of static pages and other content.

- **Static Screens and Printed Reports** – Agencies will be able to share information through the publishing of static screens. Static screens display content in HyperText Markup Language (HTML) and are delivered to a web browser using HyperText Transfer Protocol (HTTP). This information is not

dynamic, therefore it cannot be changed due to user input. The ability to publish agency reports on the web is an efficient form of information dissemination. Agency reports can be published in HTML as well as PDF formats using the appropriate "plug-in" software. Authorized users can download these published reports.

- **Threaded Discussion Groups** – Discussion groups further enhance information sharing by allowing inter-agency interaction. Discussion groups allow authorized users to post messages for response by other authorized users or data administrators.

- **Notification Services** – Notification services enable data to interact with authorized users. This level of information sharing goes beyond the others and allows certain changes in data to be pushed to specified users.

- **Core Data Transfer** – Data transfer is the pinnacle of information sharing. Data Transfer functionality consists of redundant data being either pushed or pulled from the data originating agencies to other subscribing agencies. This reduces human intervention involved with the entry of data into agency systems, hence reducing the probability for errors that can promulgate and lead to reduced data quality.

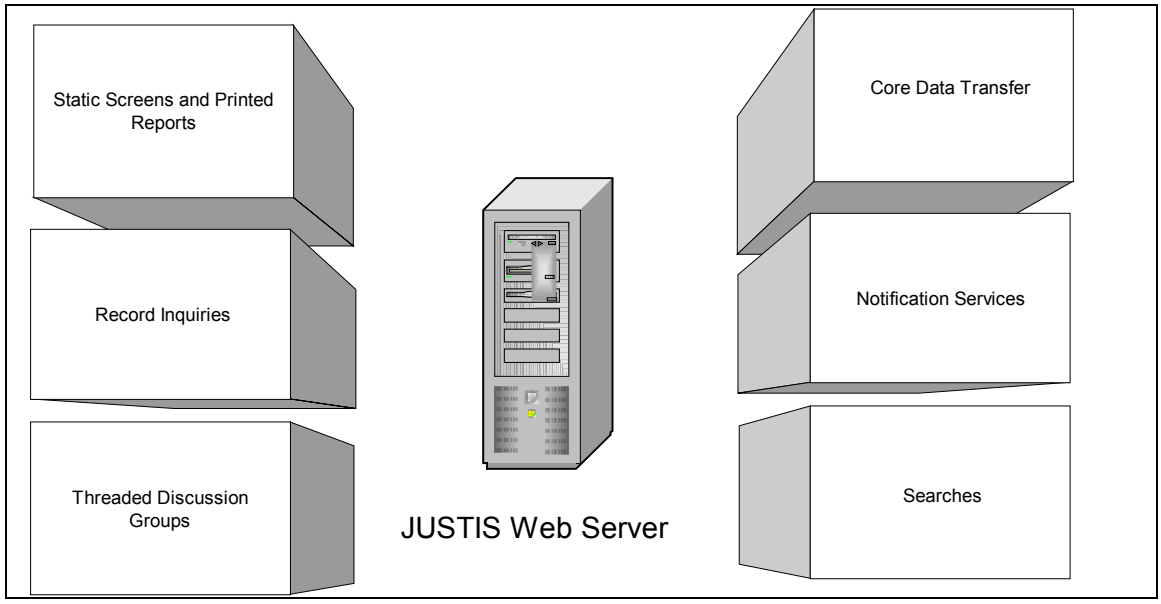


Figure 4 – JUSTIS Information Sharing Modes

Information sharing will be made possible through the use of a secure justice system-wide Intranet. Through JUSTIS, community agencies will each be able to have a unified view of justice information. This unified view is currently not possible because each agency's legacy system holds an individual island of information.

JUSTIS connects these islands into a unified system available to answer user queries. This section details the data each agency has chosen to share.

Subsequent sections will provide details on the modes of searches, static screens and printed reports, threaded discussion groups, secure email and notification services. The remainder of this section provides details on the JUSTIS query applications (referred to as Criminal Justice Inquiry or CJI).

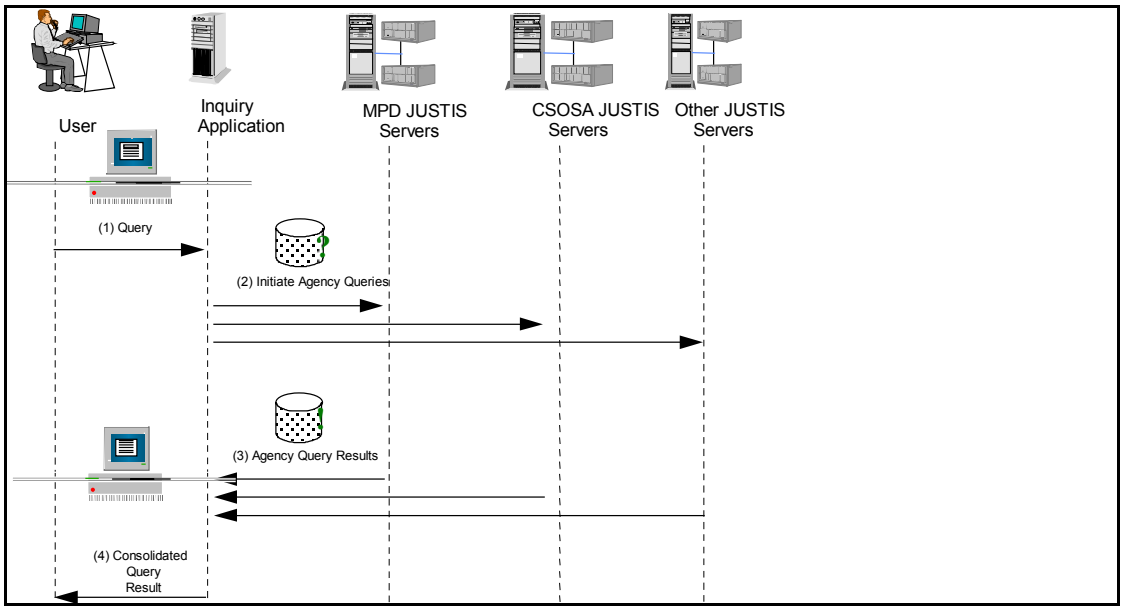


Figure 5 – JUSTIS Inquiry Application Flow

The JUSTIS inquiry application provides a justice worker with data from justice agency sources via a single-point search application and user interface. Typically, the data sources will reside in databases controlled by individual agencies.

Search results are organized in a file and folder metaphor. The architecture of this application must allow for the ability to incorporate new types (documents) and new sources (agencies) of information as they come on line, without having to be rewritten or requiring extensive re-configuration. It must also be able to restrict access to information found by the search (at least on a document level, if not on a field level).

Individual agencies determine information to be shared and decide upon mechanisms for which JUSTIS will acquire the shared data. Information detailing each agency's selected data contribution methodology is documented in JUSTIS Phase 2 deliverable 4.1, JUSTIS Data Contribution Design Document. This document lists a description of the data each contributing agency has agreed to share through JUSTIS, provides an illustration of the technical design of the data transfer and concludes with the entailing process involved with the agency data contribution.

The JUSTIS contributing agencies that are included in deliverable 4.1 are as follows:

- Court Services and Offender Supervision Agency (CSOSA)
- District of Columbia Department of Corrections (DCDC)
- District of Columbia Superior Court (DCSC)
- Metropolitan Police Department (MPD)
- Office of Corporation Counsel (OCC)
- Pretrial Services Agency (PSA)
- United States Attorney's Office (USAO)
- United States Parole Commission (USPC)
- Youth Services Administration (YSA)

As a result of the successful implementation of JUSTIS, agencies outside of the CJCC have requested access and the ability to contribute data. This will build upon the agency expansion accomplished in Phase 2. During future phases, JUSTIS will invite the United Sates Marshal Service (USMS) to have access only, the Federal Public Defender (FPD) to become a contributor and to have access, the United States District Court (USDC) to become a contributor and to have access, the Federal Bureau of Prisons (BOP) to have access only, and the Department of Motor Vehicles (DMV) to become contributor only.

3.2.1 *Agency Data Sharing*

The CJCC member agencies have coordinated with the ITLO in developing an Agency Data Access Matrix. This matrix summarizes the data accessibility of user agencies as defined by the contributing agencies. This matrix will be the basis on which group access is granted.

Interagency Contribution / Access Chart

Agency Providing Data — **Access Allowed to Others by the Providing Agency**

	BOP	CSOSA	DCDC	DCSC	MPD	OCC	PDS	PSA	USAO	USMS	USPC	YSA
BOP		N/A_a	N/A_a	N/A_a	N/A_a	N/A_a	N/A_a	N/A_a	N/A_a	N/A_a	N/A_a	N/A_a
CSOSA	YES		YES	YES	YES	NO	NO	YES	YES	YES	YES	NO
DCDC	YES	YES		YES	YES	YES	YES	YES	YES	YES	YES	YES
DCSC	YES	YES	YES		YES	YES	YES	YES	YES	YES	YES	YES
MPD	YES	YES	YES	YES		YES	YES	YES	YES	YES	YES	YES
OCC	YES	YES	YES	YES	YES		YES	YES	YES	YES	YES	YES
PDS	YES	YES	YES	YES	YES	YES		YES	YES	YES	YES	YES
PSA	YES	YES	YES	YES	YES	YES	NO		YES	YES	YES	YES
USAO	YES	YES	YES	YES	YES	YES	YES	YES		YES	YES	YES
USMS	N/A_b	N/A_b	N/A_b	N/A_b	N/A_b	N/A_b	N/A_b	N/A_b	N/A_b		N/A_b	N/A_b
USPC	YES	YES	YES	YES	YES	NO[1]	NO[1]	NO[1]	YES	NO[1]		NO[1]
YSA	NO	NO	NO	YES	NO	YES	NO	NO	NO	NO	NO	

Legend

YES = Access is permitted

NO = Access is NOT permitted

Restrictions

[1] Pending review of access request

N/A_a = Non-participant

N/A_b = No data Contribution

3.3 Summary of Data Contribution

The following table summarizes the data that agencies have discussed sharing and the data that other agencies have expressed a particular interest in.

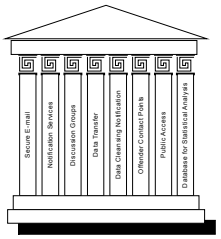
Data Category	Metropolitan Police Department	CSOSA	Superior Court of the District of Columbia	District of Columbia Department of Corrections	Federal Bureau of Prisons	Office of Corporation	Public Defender Services	Pretrial Services Agency	United States Parole Commission	United States Attorney's Office	Youth Services Administration
Identification Data	♣										
Arrest Data (PD163)	♣	♦	♦	♦					♦	♦	♦
Sex offenders	♦										
Correction Information	♦										
Charge Data		♣									
Pretrial Release Status		♣						♣			
Warrant Data		♣									
Parole Length Data		♣									
Parole Violations		♣									
Pretrial Drug Test		♣									
Case Scheduling Data			♣								
Charge Data			♣								
Sentencing Data			♣								
CJIS Data			♣								
USAO Data			♣								
Lockup List			♦								
Location Information			♦								

Data Category	Metropolitan Police Department	CSOSA	Superior Court of the District of Columbia	District of Columbia Department of Corrections	Federal Bureau of Prisons	Office of Corporation	Public Defender Services	Pretrial Services Agency	United States Parole Commission	United States Attorney's Office	Youth Services Administration
Mug Shots			♦								
US Attorney Assignment			♦								
Inmate Location				♣							
Institutional Infraction				♣							
US Courts Data				♦							
DC Courts				♦							
Final Decision Data									♣		
Pretrial Data								♣	♦		♦
Per-Sentence reports									♦		
Case Assignment Data						♣	♣				
PD251		♦								♦	
Pretrial Current Status								♣		♦	
Pretrial Condition of								♣		♦	
Probation Officer Data		♣								♦	
Social File Number Data											♣
YSA File Number Data											♣
Court Disposition Data											♦
Juvenile Probation Data											♦

♣ – Contributed Data

♦ – Agency Expressed Interest in this Data

3.4 Other Interagency Functions Supported JUSTIS



The previous section described the core functionality of information sharing within JUSTIS. This section discusses the individual functions that further enhance the system and empower its users to fully collaborate with one another.

3.4.1 Notification Services: Publish and Subscribe

The future JUSTIS system will be designed to allow events within the JUSTIS to trigger notifications to interested and subscribed parties. The notification could be on an individual basis or a group basis. For example, when a parolee is arrested and booked, this event (the police booking) can generate a notification to a parole officer or group of interested parties. This section of the Blueprint will define major events and those who have expressed an interest in notification.

Below is a summary of the possible events and the originating agency that will be trigger the notification.

Event	Originating Agency
A new arrest	Pretrial Service Agency
An escape	District of Columbia Department of Corrections
A release from incarceration	District of Columbia Department of Corrections
Change of attorney assignment	District of Columbia Superior Court
Change of court date	District of Columbia Superior Court
Disposition of trial	District of Columbia Superior Court
Issuance of warrant	District of Columbia Superior Court

There is no Notification related system currently in existence. In order to implement JUSTIS Notification system the following task has to be implemented. The Notification system will be designed around the concept of publish and subscribe as depicted below.

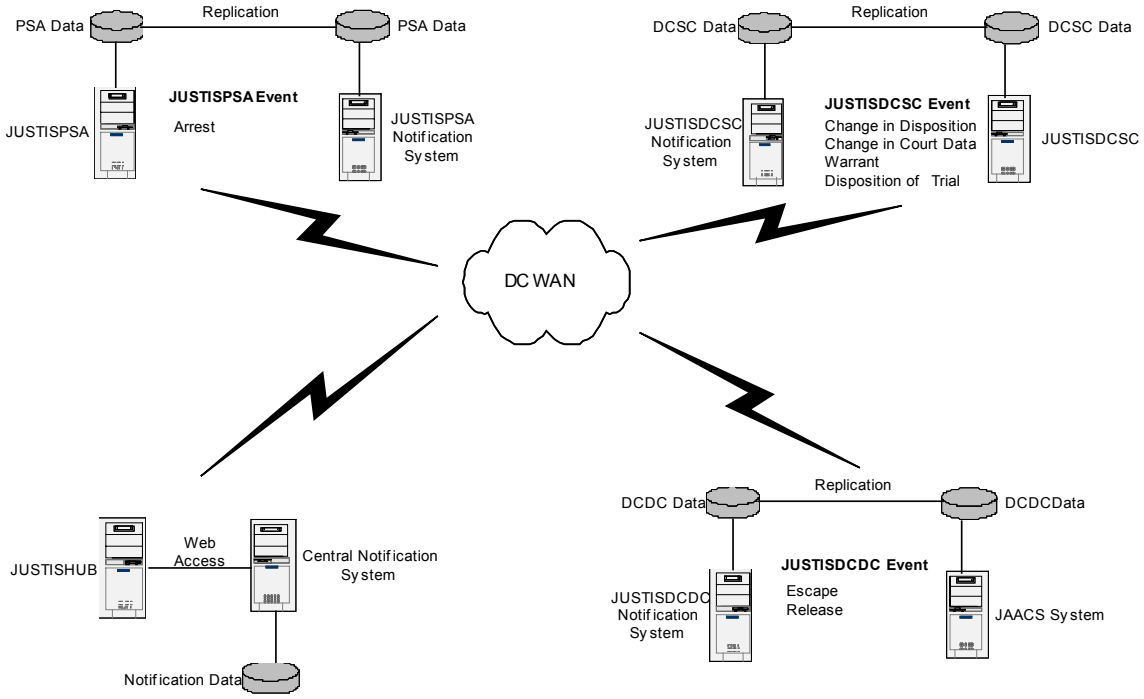


Figure 6 - Notification Services Design

3.4.1.1 Subscriptions:

Users will decide the events for which they will receive Notifications. Through a user-friendly interface, they will configure the notification system to receive these events (Subscription of events).

The system will present a web page to the authorized user that allows the user to subscribe to events and to list the specific details of the subscription. Details include: duration, number of occurrences, specific keys. For example, a user could subscribe to all arrest event notifications that occur on or before 12/31/2003, are the first arrest or a repeat request for PDID 123456.

3.4.1.2 Delivery:

Web notification will be accessible via the JUSTIS web-based interface. A special web-based application will be developed for notification system users. When users log on, a list of new notifications will be displayed for his or her examination. A new event will either redirect the user to the notification system or pop up an alert that a notice is waiting for them.

The design of the notification system will be modular in nature. During this task, web browser notification will be available. Future stages may have e-mail notification, pager notification or voice mail notification. Adding these types of delivery to a modular system design should mean that the majority of the existing code will be unaffected. Only new modules and interfaces need to be implemented.

3.4.2 Collaborative Services: Discussion Groups

JUSTIS provides the environment for threaded discussion groups/forums. A discussion forum is an on-line conference. A JUSTIS system administrator can set up discussion forums, and any other authorized JUSTIS user with a web browser and the proper access can join in and participate in the forums. Unlike Newsgroups, which are open to the public, threaded discussion groups/forums are only available to authorized users. This on-line forum allows users to:

- Discuss topics of mutual interest.
- Ask questions of anyone in the forum.
- Search through message archives by keyword.
- Accomplish the data cleansing notification system through a discussion group.
- JUSTIS technical help desk questions could be fielded through a discussion group. This would allow both the users and the technical resources to search and review the group's archives for answers to frequently asked questions.

Discussion groups promote a sense of community among members. This capability therefore ties back directly to the JUSTIS business objective of promoting collaboration.

Threaded discussion groups are different from on-line chat. On-line chat takes place in real time, which requires that all participants who want to communicate be logged in and typing at the same time. This makes for a distracting and difficult-to-follow conversation. Threaded discussion groups allow authorized JUSTIS users to view ongoing conversations, post messages to those conversations, and create new conversations at any time convenient to them.

Another difference between on-line chat and threaded discussion groups is that, in on-line chat, once everyone logs off of the chat forum, there may be no record of the conversation. Discussion groups post messages into a discussion database. This allows users to post new messages and view other user's recent and past messages whenever desired. This also allows messages to be indexed and users to search for messages by keyword or other criteria.

Threaded discussion groups are also different from electronic mail. In email, a user's inbox is private to that user. In a discussion group, all members of the group (sometimes referred to as a forum) can see and respond to all messages. The discussion group becomes, in effect, a community in-box.

Discussion groups can be moderated or non-moderated. In a moderated group, a moderator is selected and given special access privileges. When a user posts a message to a moderated group, the message is not made available to the group until the moderator has approved the message for distribution.

The following is an example of the introductory interface of a discussion group:

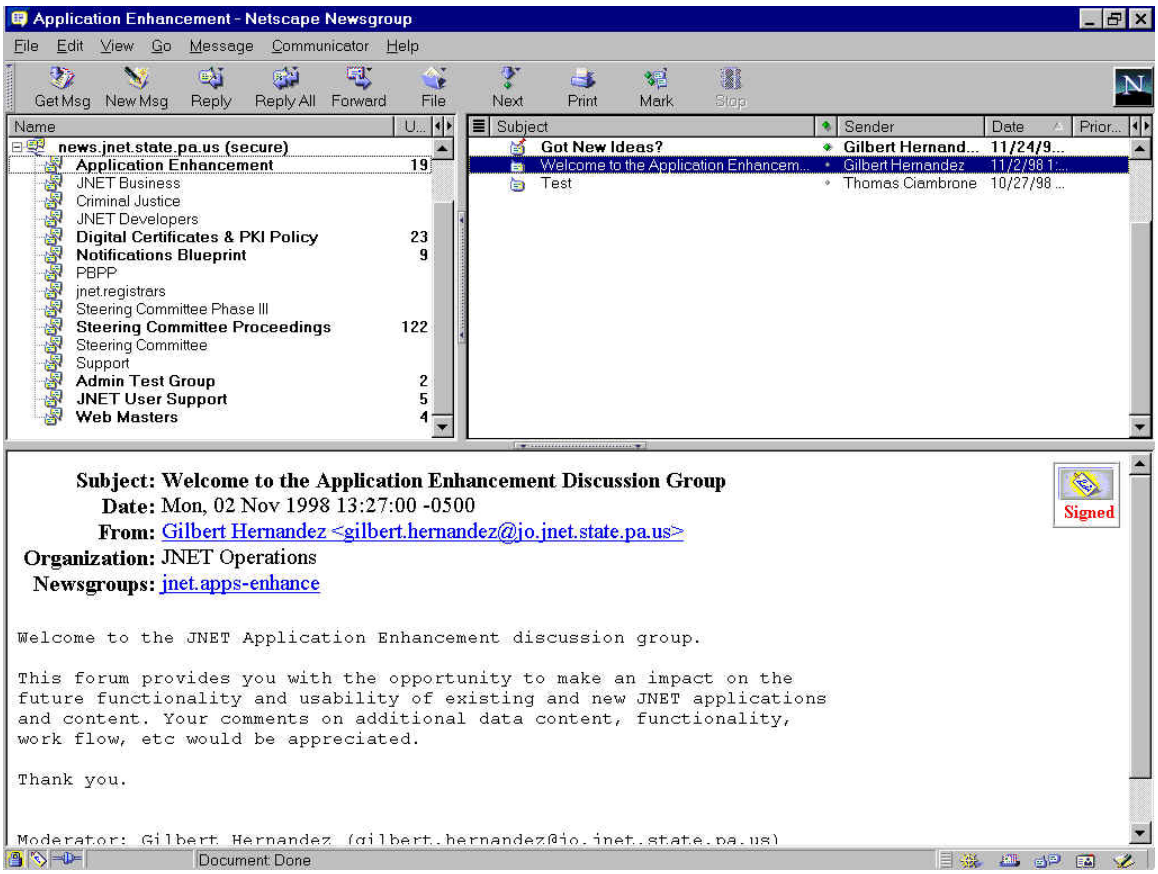


Figure 7– Screen Capture of a Discussion Group

3.4.3 *Data Transfer*

This functionality will be developed based on joint analysis and design (JAD) sessions with the CJCC, OCTO, the ITAC and its working groups. Therefore, the design below is preliminary until an agreed upon approach is developed through the JAD sessions.

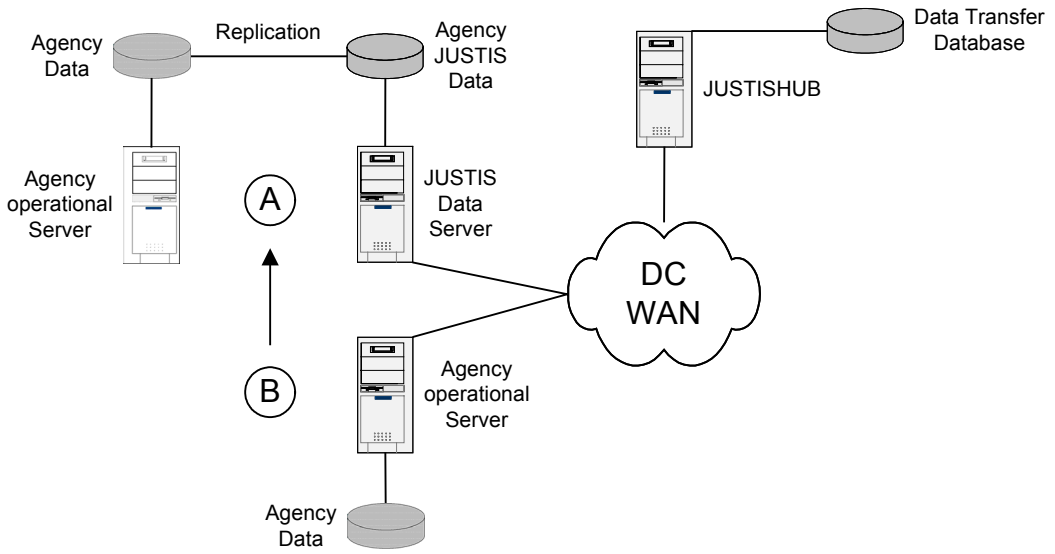


Figure 8 - Type B Agencies Will Need to be Changed to Type A

for Phase 3 Data Transfer

3.4.3.1 Creation of Core Data

As depicted in Figure 8, JUSTIS Agencies during Phase 2 have made their data contribution in one of two ways. In Type A (MPD, PSA,DCSC, etc.), a JUSTIS Data Server has been deployed for the agency and the agency's operational data is replicated in some fashion from the operational system into the JUSTIS system. Replication occurs through indirect, batch export and import or through direct database mirroring. Replication can be immediate or delayed on a weekly schedule.

Type B data contribution (USPC, DCDC) is direct to the JUSTIS Inquiry Application, with no intermediate data server. Type B connections are real-time in nature. This type of arrangement offers less flexibility to functionality such as data transfer.

In order for JUSTIS to continue to recognize the primacy of agencies over their systems and data and in order to continue to minimize the impact JUSTIS has on agency legacy systems, changes to each type of connection may be required.

For Type A connections to support data transfer functionality the replication schedule needs to be rapid – between real-time and every fifteen minutes. This is because the need for data within the transfer paradigm is almost immediate. For example, a police booking's information may be required by Pre-trial Services within minutes of the booking taking place.

Type B connections will either need to be changed to Type A or the operational system itself will be required to send messages upon an admissions protocol being conducted. In the latter case, either this functionality exists in the agency's system or it will need to be created. This will require agency system modification to accommodate the messaging functionality.

For creation of core data in this task of JUSTIS Phase 3, two agencies are considered as data originators. These are MPD and PSA. While both agencies are currently Type A, modifications to each agency's phase 2 infrastructure will be required.

At MPD, arrest records are currently planned to be transmitted to the JUSTIS data server on a weekly basis. Since it is these arrest records that need to generate core data for transfer, the timeliness of replication will need to be dropped to at most every 15 minutes.

Due to the proprietary format of the arrest information and MPD's on-going implementation of new systems, MPD presents special challenges. The recommended approach at present would be for MPD to modify its Wales system to issue a new record into a transaction file with each new booking

Without MPD, for arrests to initiate data transfer PSA becomes the next logical option. PSA also presents challenges and are also migrating to new systems. Currently, PSA's data contributory system is a Type A application running on an AS/400, with replications taking place only weekly. The new system will be based on SQL Server, and should thus allow real-time replication.

The suggested design is therefore to work on all aspects of this system simultaneously and to work closely with PSA and MPD to be ready for their new systems. PSA should be ready first and should be operational within the time period of JUSTIS Phase 3.

The production of core data upon admissions protocol exercised at PSA will work as follows:

- The PSA JUSTIS Data Server (JDS) will be a real-time replication of the PSA Operational System database.
- The JDS will be coded to include triggers in the database that fire when a new arrest is recorded or a change to an arrest record's core data is recorded. These triggers will be based on at least one of the following: PDID, arrest number or common tracking number (if implemented).
- When a JDS trigger fires, the core data elements for the new or changed record will be placed into an XML payload. The XML data will be converted to the agreed upon standard format (e.g. NCIC2000).
- The XML payload will be sent to the JUSTISHUB for addition to the data transfer database (as depicted in Figure 8).

The design of the XML payload, the triggers, the processing software and the schema of the data transfer database will be extensible to other agencies such as MPD. Once these agencies' systems are ready for near real-time replication, addition of them into the core data transfer process should be mostly a matter of coding the triggers at that agency's JDS.

3.4.3.1.1 Consumption of Core Data

Once the data is transferred to the data transfer database, it is stored in XML format as is available to any consuming agency by either "push" or "pull" technology.

Consumption by Pull

The JUSTIS web site will have an application added to it that allows authorized users (as determined by their access control list maintained in the LDAP directory) to:

- Search the data transfer database with a variety of keys (PDID, Last Name, Arrest Number) and a set of sorts and filters (date of origination, originating agency.
- As in the main JUSTIS Inquiry Application, the data transfer application will allow the return of a single record (e.g. last night's booking information for John Doe with arrest number 123456) or a group of records (e.g. all of last night's bookings sorted by last name alphabetically).
- Once a record or records are returned, the user will then have the ability to:
  - Cut and paste fields from their web browser window into other windows based applications.
  - Select a button to download the record(s) in XML format.
  - Select a button to download the record(s) in Excel 2000 format.
  - Select a button to download the record(s) in Access 2000 format.
  - Select a button to download the record(s) in a comma delimited, flat file format.
- Once downloaded, it is the user's responsibility to import or cut and paste the information into the agency's operational system. The user may need to transform the data from its stored format (e.g. XML/NCIC2000) into the format used by the operational system.
- The JUSTIS dissemination logs will be modified to include data transfer activity.

Consumption by Push

The JUSTIS system will have an application added to it that allows authorized agencies and their systems (as determined by their access control list maintained in the LDAP directory) to be sent ("pushed") core data. Details of this system design include:

- The agency will "subscribe" to the type of data they wish to be pushed to them. Subscription information includes: originating agency, date range of records and frequency of push. For example, PSA might subscribe to the MPD arrests for the previous day.
- Records will be transmitted in a secure, standards based protocol such as SHTTP or SSL encrypted FTP.
- The transmitted records will be formatted in one of the following standards: XML, Excel 2000, Access 2000, or a comma delimited, flat file format.
- Once transmitted and placed on an Agency server, it is the agency's responsibility to import the information into the agency's operational system. The user may need to transform the data from its stored format (e.g. XML/NCIC2000) into the format used by the operational system.

3.4.4 Data Quality Alliance

The implementation of a system whereby related information from different sources can be viewed requires a business process that resolves data inconsistencies. By pulling together multiple agencies' views of data through JUSTIS, inconsistencies might be noted. JUSTIS currently accommodates a business process whereby the user sends a report via email of inconsistencies or suspected errors to another agency's data quality administrator. The data quality administrators from the different agencies coordinate a resolution to the data inconsistency. For example, a user retrieves data from MPD that displays an offender's charge number. This same user notices that the data retrieved from Pretrial Services Agency displays a different charge number. The user could then send an email to the data quality administrator of both systems requesting them to verify the data and correct it accordingly.

During future phases of JUSTIS, the users will receive added functionality with regards to data quality assurance. This will be developed via joint analysis and design (JAD) sessions with the CJCC, OCTO, the ITAC and its working groups. This section provides a conceptual solution that could be implemented and provide functionality that would contribute to the agency's data quality alliance.

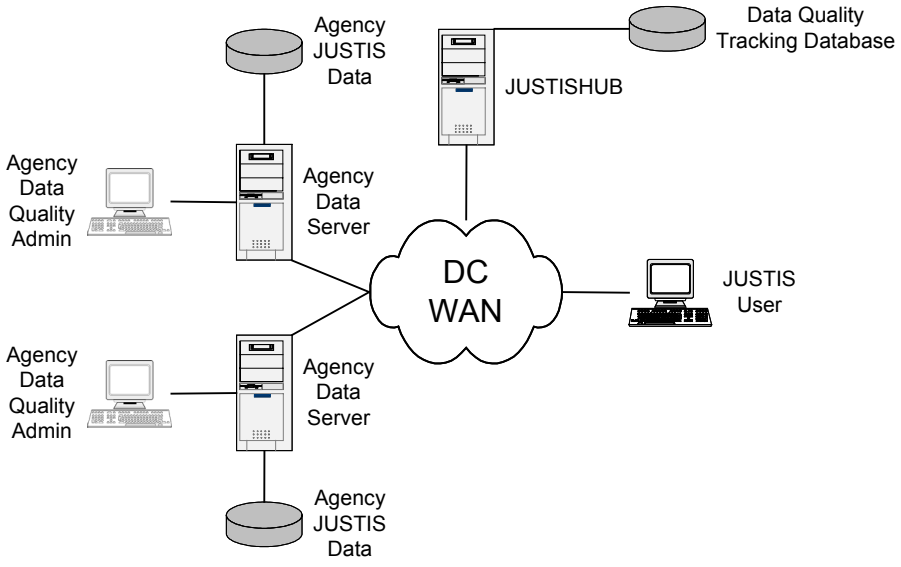


Figure 9 – Data Quality Alliance Schema

3.4.4.1 Noticing a Data Quality Issue

The JUSTIS system, because it does not collect data, cannot discover data quality issues automatically. Rather, JUSTIS users are the vehicles through which errors and cross-agency inconsistencies are noticed. This user-discovery comes with normal usage of the system.

In addition to a user being the first one to notice a problem, the JUSTIS data results screens will be modified to include a button to “view data quality reports”. This button will be present and enabled on screens that show data for which an earlier data quality report has been issued.

3.4.4.2 Reporting a Data Quality Issue

When a user notices a problem with the data, the user clicks a button on the error page in question. Note that this button and its processing is not yet part of JUSTIS and will need to be added. The “submit data quality alert” button will open up a web browser window where the user can fill in the report. The report will pre-populate with the user’s name and userid, the date, the time, the query parameters the user entered, the agency and dataset being reported, and the entire contents of the web page (agency data results) being reported.

The user will have a textbox area in which to type the nature of the problem and any recommendations for action.

If this is not the first report to be issued on this data, subsequent users will be allowed to enter their comments into a textbox and these comments will be appended to the original report. In this manner, a history file is maintained on the data quality reporting process.

3.4.4.3 Tracking Data Quality Issues

Each time a data quality report is created by the user, a record is created in a SQL Server database. This database – the "data quality tracking database" in the diagram above – is maintained on the JUSTISHUB server.

The database tables will contain at least the following information for each data quality report: the agency, dataset and key(s) of the suspect data; the reporting user, date and time issued; a copy of the HTML page from which the user reported; the data quality administrator (DQA) responsible for addressing the problem; additional user comments; additional DQA comments and a status code.

Various web based reporting mechanisms will be developed for the database. This will allow JUSTIS administrative and management staff to run reports such as all open problems by agency and by age of report. If it proves necessary, JUSTIS administrators can send these reports to agency DQA's to request action and resolution.

3.4.4.4 Resolving Data Quality Issues

When a DQA logs into JUSTIS, the system will take a special processing path. Each DQA will be directed to a summary page of open data quality reports for the DQA's agency. The DQA will be tasked to review these reports on a routine basis and to take corrective action. Because JUSTIS is not storing the agency's data, this corrective action must ultimately be on the agency's operational system.

For example, should PSA discover through user reporting that they have an incorrect address for a given individual, the DQA should first verify the correct information and should then update the operational system at PSA. The DQA would then update the data quality report on JUSTIS with appropriate comments and change the status to indicate the problem has been resolved and closed.

3.4.5 Public Access

Remaining cognizant of the guiding principles of the ITAC, JUSTIS provides the opportunity to "nurture agency and community requirements for research and

public access." This principle allows the public to recognize a tangible value from JUSTIS. The methodology for publishing data to the public will be exceptionally secure and "one way." JUSTIS will publish data in a static format and reports in PDF format that will allow accessibility to the public. As stated before, static format and PDF formats are non-dynamic and cannot be changed due to user input.

The final solution for providing public access will also be developed based on joint analysis and design (JAD) sessions with the CJCC, OCTO, the ITAC and its working groups. Nevertheless, this section describes a possible solution for providing public access functionality.

Upon completion of the development of this functionality, the current CJCCDC.org web site will provide a public portal of available data regarding offenders. This system will remain separate from the secure JUSTIS solution. Therefore this option installs a web server and populates it with the cjccdc.org web site content as well as links to DC Justice Agency publicly available information. This web "portal" will be in the DC OCTO web development standard.

Figure 10– CJCCDC Internet Site Public Access

3.4.5.1 Maintaining CJCCDC Public Access web site

The CJCCDC Internet site serves as an information gateway for the citizens of the District of the District of Columbia. The web site uniquely supports participating agencies efforts to provide the public with timely information.

Maintaining the CJCCDC Internet site consists of working with agencies to determine the extent of public accessible data and reviewing DC Web kit design standards with agency webmasters. Participating agencies benefit by increasing their ability to share information with the public. Due to the web site's ability to provide public access to multiple agencies, the CJCCDC Internet site functions as a threshold to bridge individuals affected by the criminal justice system and agencies serving the citizens of the District of Columbia.

3.4.5.2 Creating Advanced Portal Infrastructure for the CJCCDC Internet site

The key tasks needed to achieve successful implementation of a public web portal include:

- Researching appropriate links
- Contact agencies to request linking from www.cjccdc.org to designated agency website(s)
- Develop content and infrastructure to populate web site portal
- Test and deploy the portal

3.4.6 Database for Statistical Analysis

The final solution will also be developed based in joint sessions with the CJCC, OCTO, the ITAC, the SAC Director, DCSC, DCDC, DCFES, CSOSA, USAO, MPD and PSA. This section presents an initial solution that provides the reader a conceptual description of a possible solution.

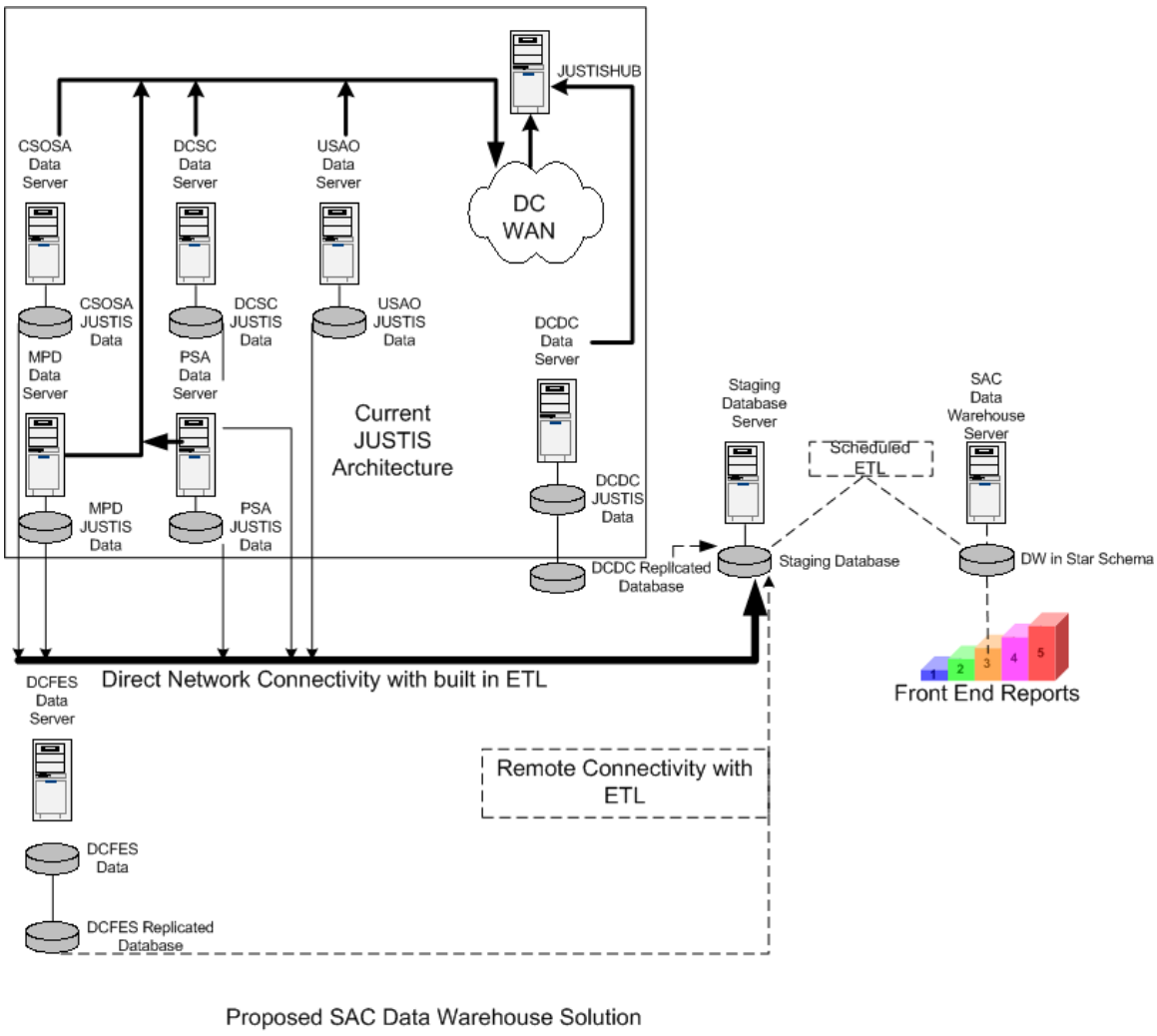


Figure 11– Proposed SAC Data Warehouse Solution

3.4.6.1 Figure 1:Proposed SAC Data Warehouse Architecture

The current JUSTIS implementation pulls data on a scheduled basis from MPD, DCSC, CSOSA, PSA and USAO and directly connects to DCDC's data. DCFES data is not included in the current JUSTIS structure.

In order to provide SAC with parallel access to JUSTIS data, it is suggested ETL (Extract, Transform and Load) programs be developed to pull data from the agencies that currently provide data on a scheduled basis. These agencies are CSOSA, DCSC, USAO, MPD and PSA.

A different set of ETL programs should be developed to pull data from replicated DCDC and DCFES databases. Since these databases normally provide data to the JUSTIS framework directly, going against replicated databases will have no impact on functional agency systems.

Two servers configured to serve as a specialized Staging Database Server and a SAC Data Warehouse Server must be procured initally. The Staging Database Server will store the results of the data extracted, transformed and loaded from the agencies of interest to the SAC Warehouse. The SAC Data Warehouse Server will contain the actual Data Warehouse and front-end reporting tools.

Network connectivity between the JUSTIS databases of MPD, DCSC, CSOSA, PSA and USAO and the Staging Database Server must be designed and implemented in order to facilitate ETL between these databases and the Staging Server.

Also remote network connectivity between the replicated databases of DCDC and DCFES and the Staging Database Server for ETL purposes must be designed and implemented. All network connections must conform to the JUSTIS security requirements. This may require additional cryptographic hardware and software to be procured.

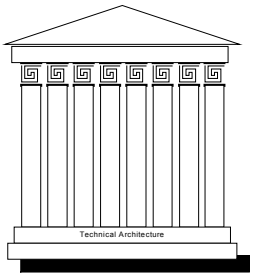
ETL programs must then be developed to move data from the Staging Database Server to the SAC Data Warehouse Server to conform to a Star Schema design that must be developed for the Data Warehouse.

Finally, a reporting solution and/or multi-dimensional analysis solution must be designed and implemented on the Data Warehouse Server for SAC.

The overall purpose of the proposed architecture is to ensure that:

- The SAC system will not interface or interfere with JUSTIS
- Only data relevant to the needs of the SAC will be provided from DC Agencies
- All SAC functions can be carried out on the Center's own Hardware and will utilize its own communication facilities
- The SAC can meet all its reporting needs as mandated by its Executive Order with the least possible impact on agencies in the field

3.5 Technical Architecture



We have discussed the overall business requirements and system goals of JUSTIS. We then discussed the functional elements of the systems that collectively empower JUSTIS users to achieve the business objectives. This section now turns to the technical infrastructure and architecture necessary to support the functional elements.

3.5.1 Full Security Implementation

The JUSTIS security architecture is modeled after the World Wide Web. Information to be shared will be "published" by its owner agency on distributed JUSTIS Agency Servers, and authorized agency personnel can access JUSTIS server content using web-browser software on a desktop computer. A Hub Server will provide a shared platform for centralized applications, agency-independent content, and inter-agency communication.

Unlike the web, however, JUSTIS will be a secure Intranet. Firewalls will protect the network from unauthorized access. Encryption and digital certificates will provide secure communication and user/server authentication.

The JUSTIS network will be a cooperative and collaborative environment in which many users of the network are interacting at any given time. This interaction requires a strong and flexible layer of security to provide protection to communications over the network and to data stored on the legacy systems.

Security is a collection of technologies and policies that enable JUSTIS to provide and deny access to system resources on a controlled and consistent basis. Security protects the system resources, which can be either physical (network) or informational (application).

The design of the JUSTIS security implementation is fully documented in two deliverables presented during the course of JUSTIS Phase 2. The first, deliverable number 1.7 Security Policy and Procedures, provides and overview of the security policies and procedures that provide the foundation upon which JUSITS operates. This document conveys the importance of a hierarchical organizational structure in the administration of system security, provides an administrative policy, and concludes with a user access policy. Also included in the deliverable are the necessary user access forms followed by a user agreement and an access flow chart.

The second document that addresses the JUSTIS security implementation is deliverable number 1.1.2 JUSTIS Security Architecture. This deliverable addresses the technical architecture that contributes to the security implementation. It provides the user with an understanding of the objectives of the JUSTIS Security Architecture and the design and implementation of the full solution. The document communicates this through discussions of security architecture strategies, an evaluation of possible security compromising tactics and their defense, and concludes with security recommendations specific to JUSTIS along with a summary of the current solution.

3.5.2 *Overall JUSTIS Building Blocks: Web Application Development Standards*

As stated in the beginning of this Blueprint, a business requirement of JUSTIS is that it be built upon open standards and technologies. This requirement demands an approach that uses internationally accepted standard tools and techniques. Such tools are available from a wide variety of vendors. Systems developed with open technologies run on a wide variety of platforms.

The use of open technologies is important to the District and to the success of the JUSTIS System. Open technologies offer a number of advantages:

- **Vendor neutrality**. Developers who employ open standards technologies avoid locking themselves into a single vendor. This reduces project risk because a single vendor can fail to fix bugs, slip on release dates or go out of business altogether.

- **Platform independence**. Systems that are developed on open standards technologies are easier to move from one hardware platform to another or from one operating system to another.

- **Greater flexibility**. Because of vendor neutrality and platform independence, JUSTIS participating agencies will have fewer concerns about upgrading their systems and changing platforms. A JUSTIS component built to run on Windows NT and connect to a SQL Server database will require only small modifications to run on a Unix platform connecting to an Oracle database.

During the POC phase, the JUSTIS team developed the system under the Java 2 Enterprise Edition (J2EE) set of standards. The standards selected within this framework were all at an accepted level – no draft standards or vendor extensions were employed.

The specific standards used to develop and deploy JUSTIS POC System code were:

- ***JDK 1.3*** – The Java Development Kit, the Java programming language system used to develop JUSTIS application code.
- ***Java Servlets 2.1*** – Servlets are Java code that runs under the control of JUSTIS web servers.
- ***JSP 1.0*** – Java Server Pages are server-processed web pages that include programmatic Java elements.
- ***JDBC 2.0*** – JDBC is the standard access method that connects JUSTIS Java programs with back-end databases.
- ***XML and XSLT 1.0*** – The Extensible Markup Language and its accompanying style sheet language is a bundle of several related technologies. In JUSTIS, they are used to extend the power of basic web HTML pages.
- ***TCP/IP*** – Transmission Control Protocol/Internet Protocol. TCP/IP is a family of communications protocols that control traffic across the DC Wide Area Network.
- ***HTML 3.2*** – The HyperText Markup Language is what web pages are written in. The version 3.2 standard has been used to help ensure maximum browser independence.
- ***HTTP 1.1/1.0 Hypertext Transfer Protocol*** – This is the standard protocol for transmitting information between browsers and servers. HTTP is a layer above TCP in the protocol stack.
- ***SSL 3*** – ***Secure*** Sockets Layer version 3. SSL enables HTTP and other protocols to be transmitted in encrypted form across a network.
- ***X.509v3*** – ITU-T Recommendation X.509 defines an authentication framework based on digital certificates. The recommendation specifies a set of properties and content for digital certificates, as well as procedures for authentication and certificate management.
- ***X.500 Directory Services*** – X.500 is the standard for Directory Services. Directories are essentially databases optimized for read-access of network entity information. JUSTIS uses an X.500 based directory to store information about users, servers, and applications – including group membership and digital certificates – in a centralized location. The Directory Service is available to applications such as web servers and browsers that require identifying information about an entity in JUSTIS. A prime example is a web server that assigns access control to web resources based on group memberships defined in the directory.
- ***LDAP Lightweight Directory Access Protocol*** – LDAP is a protocol used by applications to communicate with the Directory. Applications are expected to utilize LDAP and the Directory to reduce the redundancy of user information on systems in a network environment.

- ***SMTP, S/MIME, POP3 and IMAP4.*** – These protocols collectively provide a secure email environment.

During Phase 2 development, the ITAC TWG and OCTO representatives reviewed the standards used throughout the District. It was discovered that in all Justice agencies, as well as in the majority of other city agencies, the server application platform most widely used for deployment was Microsoft (MS). No substantial J2EE systems, other than the JUSTIS POC, were deployed in the District in the Spring of 2001.

As a further part of this analysis, OCTO and the JUSTIS implementation team performed a cost benefit comparison of continuing with a J2EE path versus standardizing on Microsoft. This comparison showed that an MS server deployment would be less expensive than J2EE.

Therefore, recognizing that MS was the preferred platform in justice and other city agencies, recognizing that an MS deployment would be more cost-effective, and recognizing that agency participation in JUSTIS would be easier if JUSTIS used the same technologies already in use at the agencies, the ITLO and OCTO decided to refine the set of standards used in JUSTIS to incorporate certain MS technologies.

This decision had the following impact on Phase 2. First, there are a number of technologies that were used in the development of the JUSTIS POC that will continue to be the standard for JUSTIS Phase 2. These are:

JUSTIS POC and Phase 2 Standards	
Category	**Product/Standard**
Operating System	MS Windows 2000 Advanced Server
Directory Services	MS Windows 2000 Active Directory
Web Server	MS Internet Information Server 5
Web Browser	Either IE5 or NS5 or above
Browser scripting	JavaScript
Browser markup	HTML 3.2 and Adobe PDF
Database	MS SQL Server 2000
Web Page Design	MS FrontPage 2000

Secondly, a number of standards used for the POC were changed for JUSTIS Phase 2 and subsequent phases. These standards are:

Category	Phase 2 Standard	POC Standard
Server scripting	MS ASP	Sun JSP
Server objects	MS VB COM	Sun Servlets
Application Server	MS IIS 5	Allaire Jrun
Database drivers	MS ODBC	Various JDBC
Development Suite	MS Visual Studio	Inrprise Visual Studio

This change is to ease the impact that participation in JUSTIS has on its member agencies. The change to certain MS technologies assists member agencies in leveraging staff skills and software components that are already in place.

The change to server component standards does not change the basic tenet of JUSTIS to deploy open standards wherever possible. The bulk of the standards used, especially at the user interface tier, remain the internationally ratified standards. A description of the 3-Tier model JUSTIS uses and the standards in place at each tier follows.

The JUSTIS system is created on according to a classic 3-Tier paradigm. Systems built along this model are inherently more maintainable because they are functionally organized into modular components that can be individually maintained. The 3-Tiers are the user interface tier, the business logic tier and the backend database tier.

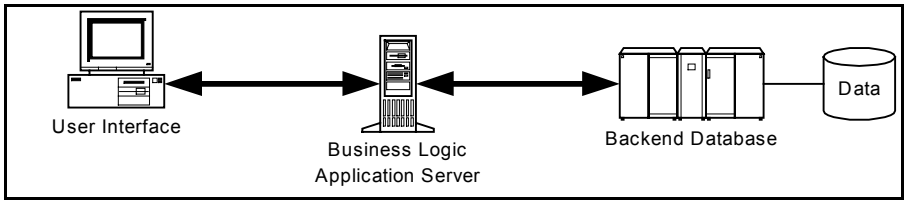


Figure 12– Three Tier Architecture

The user interface tier accepts users input (keystrokes and mouse clicks) and displays user output to the screen. In the JUSTIS model, the user interface tier is a standard web browser. Any web browser that can support HTML 3.2 will be able to use JUSTIS. Additional functionality may be delivered to web browsers that are capable of running Java applets, JavaScript and DHTML . Generally, Netscape version 4 and above and Microsoft Internet Explorer version 4 and above workstations will be able to use JUSTIS.

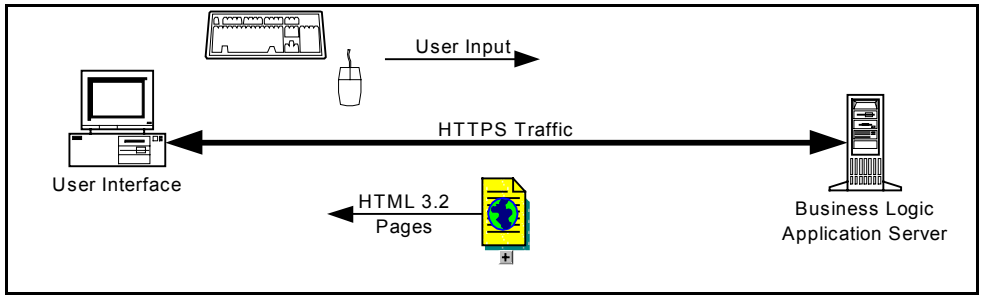


Figure 13– Communication Between User Interface and Business Logic Tiers

The business logic tier in JUSTIS is a standard web server that delivers standard web pages to the user interface tier. The business logic is built using Active Server Pages and ODBC connections to the data tier. JUSTIS is built using Microsoft IIS web server.

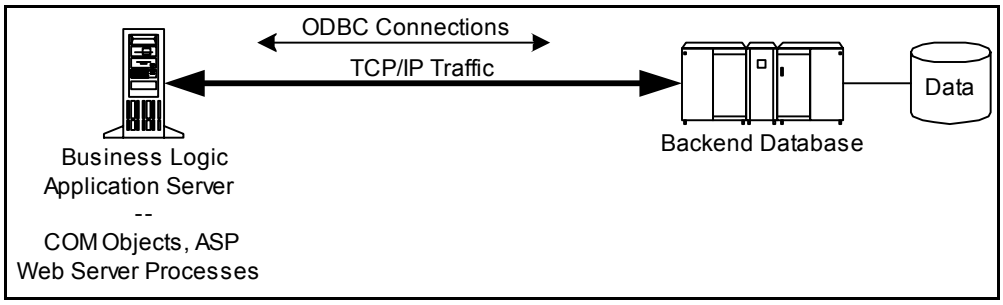


Figure 14– Communication Between Business Logic and Backend Database Tiers

The backend data tier is under the control of the participating JUSTIS agency. The use of open standards mean that this tier can change with minimal impact on the system. For example, should the database change from SQL Server to Oracle, only one line of code needs to change – the one that makes the ODBC connection

3.5.3 Physical Plant Design of JUSTIS Components

3.5.3.1 Overall Architecture

The overall JUSTIS network is a hub and spoke architecture. The hub components, described below, serve as a centralized traffic manager and offer enterprise-wide services such as email, security certificates, discussion group management and directory services.

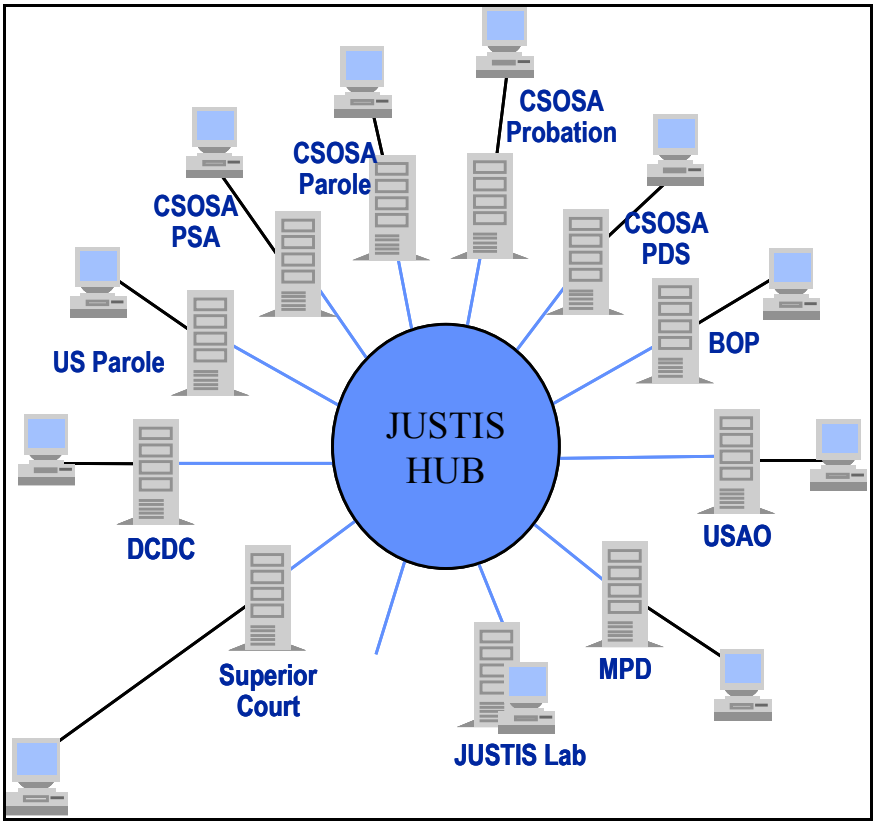


Figure 15– JUSTIS Hub and Spoke Structure

The spokes of the network are participating agency servers connected to the agency's network, user workstations, and legacy applications and data. Connections are through the DC Wide Area Network using the TCP/IP protocol.

The standards used in the design of JUSTIS leave flexibility in the selection of hardware and software. The details in this section show hardware and software choices that will be compatible with the JUSTIS architecture, but they should not be viewed as absolute requirements.

The server hardware that supports each Hub server as well as each agency server is summarized in the following table:

JUSTIS Server Configuration Specifications
Intel® Pentium® III 933MHz – 2 CPUs
1024MB Total SDRAM 133MHz (2x128, 1x256, 1x512)
Integrated Smart Array Controller (Ultra2)
Hot Plug Drive Cage

JUSTIS Server Configuration Specifications
RAID 5 setting
36GB Ultra3 SCSI 10,000 rpm Hard Drive – 3 Drives
Hot Plug Redundant Power Supply Module
1.44MB Floppy Disk Drive
10/100 TX UTP
20/40-GB DLT Drive-Internal
Windows 2000 Advanced Server
Rack Mountable R1500 UPS (low voltage 100-127VAC)

3.5.3.2 JUSTIS HUB Components

The Hub of JUSTIS contains the following servers:

- **Discussion Group Server** – this server provides central support for NNTP services. It supports JUSTIS discussion groups.
- **Certificate Server** – this server is used to assign and maintain security certificates.
- **Directory Server** – this server supports LDAP directory services. It stores user login information, security certificates, email addresses and other directory information.
- **Central Web Server** – The home page of JUSTIS resides on this server. This server serves as a central launching point for the inquiry applications, email, and access to agency web servers and discussion groups. It also provides indexed search of HTML pages and reference libraries on the JUSTIS web and agency servers, as well as search of Internet resources and static web page content such as JUSTIS news, policies, and procedures.

The software components for these servers are:

Component	Standards/Protocols	Product
Web Server	HTTP, HTML, J2EE	MS IIS V 5 with Allaire JRun Server 3
Mail Server	SMTP, S/MIME	Netscape Messaging Server 3.x
Directory Server	LDAP, LDAP API	Netscape Directory Server 1.0x

Component	Standards/Protocols	Product
Discussion Group	NNTP	Netscape Collabra
Certificate Server	X.509v3	Netscape Certificate Server 1.0x

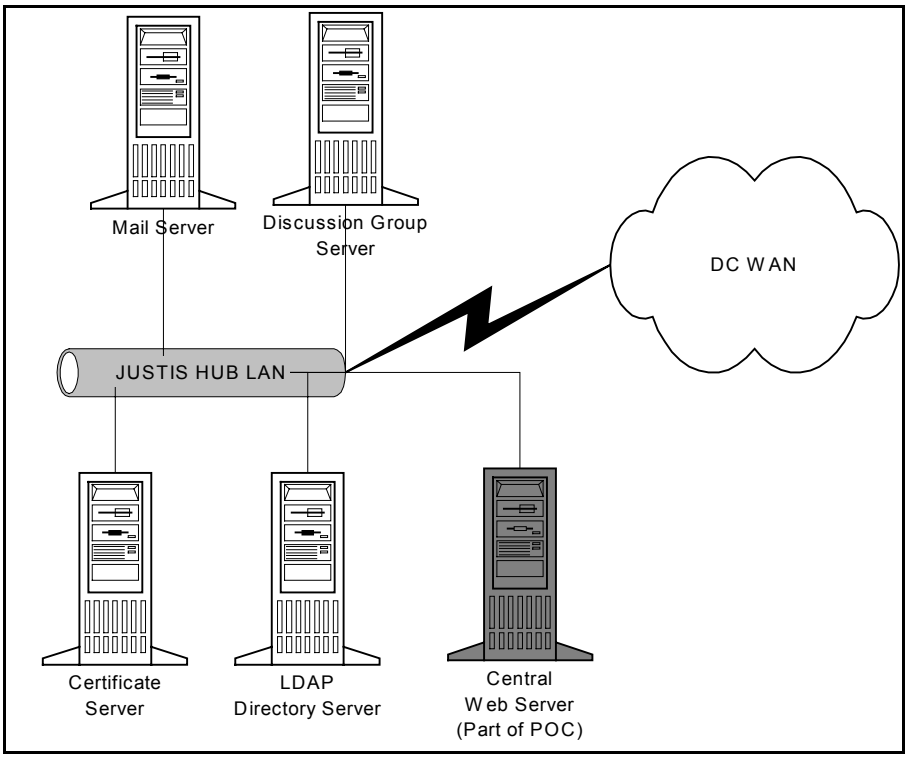


Figure 16– JUSTIS Hub Components

3.5.3.3 JUSTIS Agency Components

The participating JUSTIS agencies contain one server:

- **Agency Web Server** – The JUSTIS home page of the agency resides on this server. This server serves as the control point for the inquiry applications into the agency's legacy data.

The software components for this server are:

Component	Standards/Protocols	Product
Web Server	HTTP, HTML, J2EE	MS IIS V 5 with

Component	Standards/Protocols	Product
		Allaire JRun Server 3

3.5.4 *Scalability, Performance Requirements*

The JUSTIS proof-of-concept system is required to support fewer than 40 users. However, the design and implementation will allow for scaling to hundreds or thousands of users.

The scalability and performance improvements can be implemented on different components, these are discussed below.

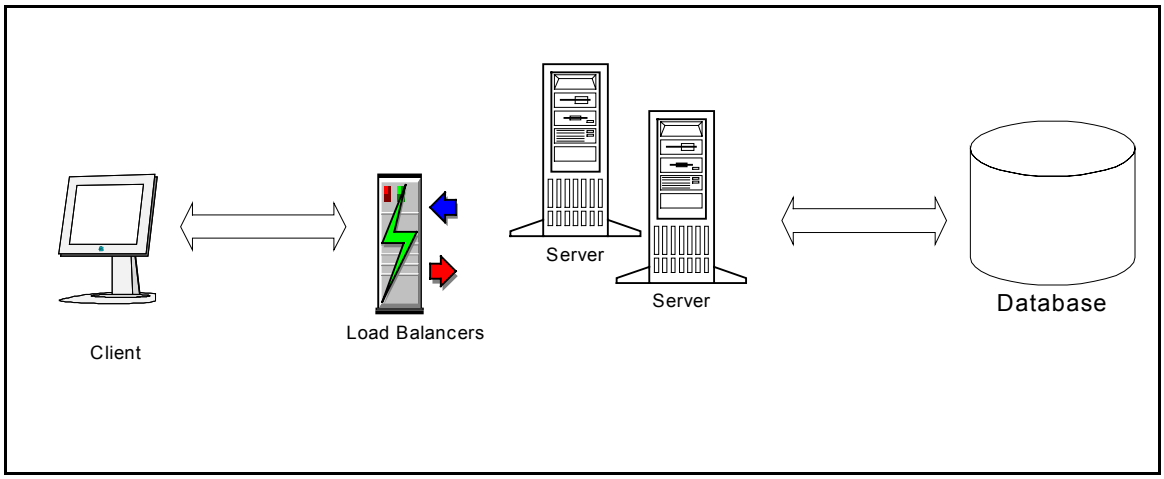


Figure 17– Areas to Examine for Performance Improvements

Component	Optimizing Technique
Client Side	On the client side, the power of the workstation can be improved by increasing the memory and the processor speed. The disk can be defragmented and the file system optimized
Load Balancers	Load balancers are used between the client and the server, so that the load is distributed equally among multiple servers.
Server	The server side performance improvements can be done be using Servlets and JSP technologies that uses only one active connection to the database for processing the clients

Component	Optimizing Technique
	request. The use of distributed computing environment increases the performance and scalability to a large extent. Java code can be written to be multi-threaded and to take advantage of multiple processors.
Database	By creating additional indexes on the tables that are queried frequently will improve the performance. Also by running the database in multi-threaded mode will improve performance.
Network	A better network infrastructure will improve the end-to-end response time. Higher speed LAN connections as well as WAN connections can be employed.

3.5.5 User Workstations

JUSTIS is a browser-based application; therefore, the system has been developed to work effectively with the following components:

- **Network** – Currently the JUSTIS POC is hosted by the District of Columbia's Office of the Chief of Technology Officer (OCTO), therefore users of the system must have a connection to the District of Columbia's Wide Area Network in order to gain access to the system. Similarly, if it is determined to develop JUSTIS on a separate wide area network, all users must have access to the network.
- **Browser** – Internet Explorer 4.0 of higher or Netscape Navigator 4.0 or higher. JUSTIS works most effectively with Internet Explorer, due to techniques employed in the District of Columbia OCTO Web Development Kit.
- **Computer Processor** – 486DX/66 MHz or higher processor.
- **Operating System** – Windows ME, Windows 95, Windows 98, Windows 2000, or Windows NT 4.0.
- **Memory** – For Windows 95, Windows 98, and Windows 2000: 16 MB (megabytes) of RAM minimum. For Windows NT: 32 MB of RAM minimum.
- **Screen Resolution** – JUSTIS is designed to be operational at all screen resolutions. A minimum resolution of 800 by 600 provides the most effective usage without the need for horizontal scrolling.

As stated before, JUSTIS is designed to be a secure intranet. This requires security components in a browser that may not be included in the version currently residing on a users' system. The users' browser is required to have

128-bit encryption strength. Future JUSTIS functionality may require cookies or JAVA applets.

3.5.6 *Network Infrastructure: Special Security Considerations*

Security infrastructure is documented in JUSTIS Phase 2 deliverable 1.1.2, JUSTIS Security Architecture, which was completed during Phase 2. This document provides readers with an understanding of the objectives of the JUSTIS security architecture and illustrates the design and implementation of a full security solution. It accomplishes this by explaining security architecture strategies, security compromising tactics and their defense, and concludes with a recommendation of a full security solution specifically for JUSTIS.

3.5.7 *Application Development Guidelines*

JUSTIS was developed using contemporary Internet technologies. The specific components used to develop applications associated with JUSTIS are documented in JUSTIS Phase 2 deliverable 1.11, JUSTIS Programming Guide. This deliverable outline the Visual Basic programming styles used throughout Phase 2 by providing a basic understanding of the structure, foundation and standards characteristic of the selected standard. It also details the utilization of webclasses throughout Phase 2, by describing the overall architecture of the objects.

3.5.8 *Off-line, Replicated, Screen-scraped and On-line Data*

Acknowledging that each justice agency is independent, it is assumed that each agency's information infrastructure and management is different. These two facts plus the additional fact that the majority of agencies manage a unique legacy system could provide an obstacle when implementing a common information system across the justice agencies. The problem centers around how will JUSTIS obtain the agreed upon shared information from the legacy system. The JUSTIS architecture provides four paradigms to choose from in order to accommodate access to agency data.

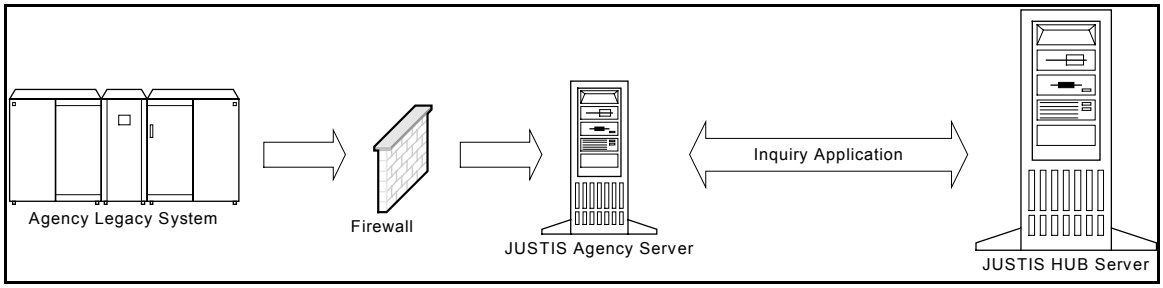


Figure 18– Direct Access

1. JUSTIS can obtain data by directly accessing, in a read-only fashion, that agency's RDBMS database. This would provide the authorized users of the system real-time data retrieval.

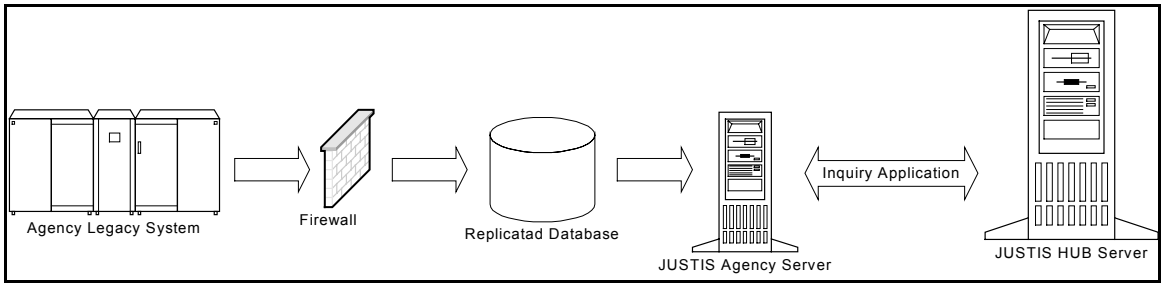


Figure 19– Replicated Access

2. JUSTIS can obtain data by accessing an agency provided replicated database. The data would be updated based upon the programmed schedule of the replicated database.

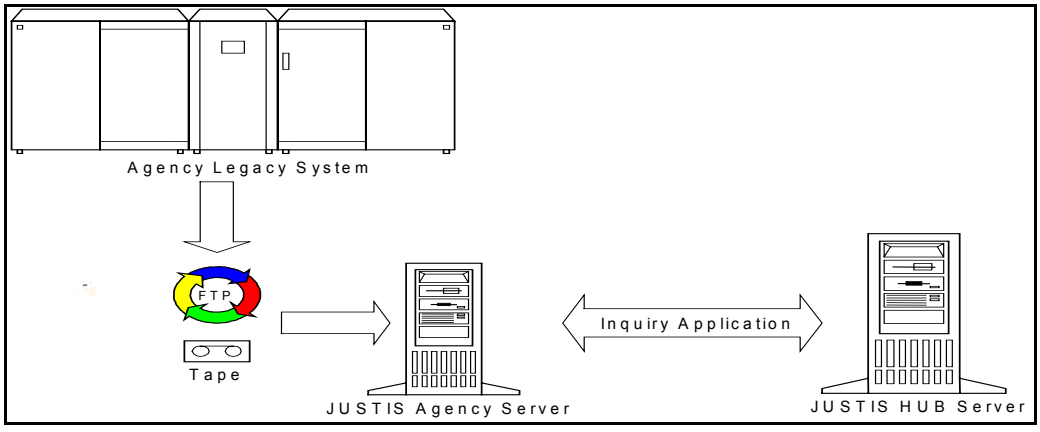


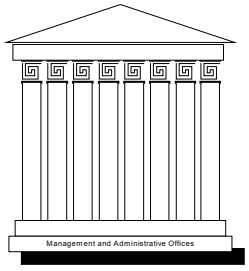
Figure 20– Off-line Access

3. JUSTIS can receive data in an off-line fashion. The data can be downloaded to tape of CD or in FTP format and loaded to the JUSTIS Agency Server. This is the most manual of the three options. This option requires active management of the data transfer. Without active management, data could become outdated, hence ineffective.

4. Finally, the agency legacy systems can be accessed in a screen-scraping fashion. In this scenario, the JUSTIS legacy connection adapter acts as if it were an on-line user of the system. The adapter sends keystrokes to the legacy application and retrieves the resulting screens. These screens are then deconstructed ("scraped") and the information is transformed into a fashion suitable for use throughout the remainder of the system.

Data Access Method	Pros	Cons
Direct Access	Real-time Data Retrieval Minimal hardware required Minimal software required	Possible legacy system performance impact Possible legacy system security impact
Replicated Data Access	Data is current Lower performance impact Lower security impact	Higher hardware and software costs Need to maintain data extract programs
Off-line Access	Lowest performance impact Lowest security impact	Data is not current Higher hardware and software costs Possible labor-intensive manual processes
Screen Scraping	Real-time data retrieval Legacy data can be in a proprietary format	Costly hardware, software and staff skills required Maintenance intensive Possible performance impact Possible security impact

3.6 Management and Administrative Structure



We have discussed the overall mission and business objectives of JUSTIS. We then discussed the functional elements of the system that collectively empower JUSTIS users to achieve the business objectives. The previous section detailed the technical infrastructure and architecture necessary to support the functional elements. We now turn to the bedrock of our future JUSTIS Blueprint – the administrative office structure required to support, maintain, enhance and promote the use of the system.

3.6.1 JUSTIS Organization Chart

The JUSTIS management and administrative structure can be summarized in the following organization chart:

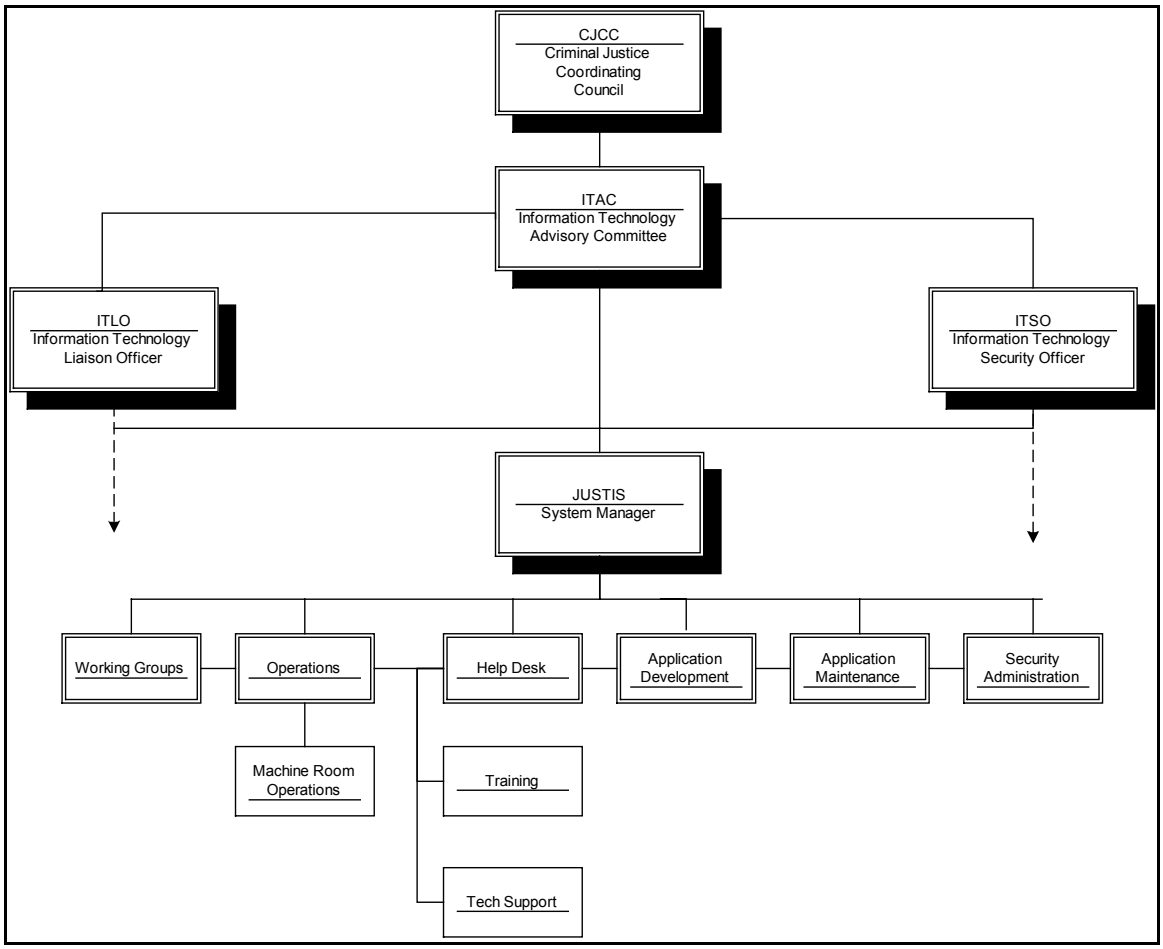


Figure 21– JUSTIS Organization Chart

The roles and responsibilities of the above organizational members are summarized as follows. These member roles and responsibilities are as they relate to JUSTIS – members have additional responsibilities outside of JUSTIS.

3.6.2 CJCC

The following is the CJCC mission statement:[3]

> The mission of the Criminal Justice Coordinating Council (CJCC) is to serve as the forum for identifying issues and their solutions, proposing actions, and facilitating cooperation that will improve public safety and the related criminal and juvenile justice services for District of Columbia residents, visitors, victims, and offenders. The CJCC draws upon local and federal agencies and individuals to develop recommendations and strategies for accomplishing this mission. Our guiding principles are creative collaboration, community involvement, and effective resource utilization. We are committed to developing targeted funding strategies and comprehensive management information through integrated information technology systems and social science research in order to achieve our goal.

One of the responsibilities of CJCC in conducting its mission is to set the overall direction and mission for ITAC. The CJCC sets ITAC's information technology mission for intra-justice agency collaboration.

3.6.3 ITAC

The ITAC's mission and goals are expressed as follows on CJCC's web site:[4]

> Mission
>
> The Information Technology Advisory Committee shall advise and recommend on matters pertaining to the funding, development, operation, maintenance and monitoring of a Justice Information System to improve public safety and the related criminal and juvenile justice services for the District of Columbia residents, visitors, victims and offenders.
>
> Our guiding principles are to:
>
> Recognize the primacy of each justice agency mission
>
> Facilitate collaborative solutions to justice information challenges
>
> Commit to the quality and integrity of justice data

[3] See HTTP://WWW.CJCCDC.ORG

[4] *Ibid.*

Implement effective data and system security

Respect the confidentiality of information and individual privacy

Establish of system-wide standards, supported by common identifiers and positive identification

Nurture agency and community requirements for research and public access

Provide for long term performance monitoring and evaluation

Goals

Encourage participation by all appropriate District and Federal justice and allied agencies at city and federal levels, including but not limited to, those on the Criminal Justice Coordinating Council

Coordinate and facilitate all aspects of the development of the Justice Information System through careful monitoring and policy decisions and by offering guidance and recommendations to the CJCC and its participating agencies

Establish and monitor ad hoc and permanent work groups and subcommittees as necessary to address the administration, funding and development of infrastructure technology, data sharing, access, integration, data and system security, system wide standards and measurement of data use and quality, as appropriate to the then-current developmental stage of the justice system

Communicate the activities and accomplishments of the ITAC, and those units it has established, and the member agencies of the CJCC

In effect, the ITAC carries out the mission it is given by CJCC and has the responsibility to:

Identify the community expansion of JUSTIS participants

Identify the functional expansion of JUSTIS capabilities

Prioritize the order of implementation of the above expansions

Monitor the implementation of JUSTIS

Manage the JUSTIS Manager

3.6.4 JUSTIS System Manager

This individual is responsible for:

- Communicating the goals and objectives of the ITAC to the JUSTIS organization
- Managing systems upgrades and implementation
- Managing system quality
- Managing system performance
- Communicating system events and status to the ITAC
- Continued monitoring of legislative actions that could affect the deployed JUSTIS system or allow for increased information sharing opportunities
- Continued monitoring of opportunities for increased system functionality
- Maintaining liaison between all JUSTIS agencies

3.6.5 *Information Technology Liason Officer (ITLO)*

The ITAC requires staff resources to for the practical day-to-day administrative activities of the Committee. This staff resource must also function as an ombudsman and liaison between the ITAC; the Executive Director of the Criminal Justice Coordinating Council, Working Group Chairs, and agencies which provide and procure fiscal and technical support such as OGMD, OCTO, the CFO and CPO. The ITLO will also communicate directly with justice agency personnel.

3.6.6 *Information Technology Security Officer (ITSO)*

In order to enforce security and carry the next critical projects forward, a key organizational stakeholder needs to be identified as the Information Technology Security Officer (ITSO). METAGroup has identified this as a critical component to successful implementation. They note that fully 58% of organizations have a central security office and a security officer who reports directly to the CIO.[5]

The Security Office promulgates security policy planning and documentation requirements and conducts the following activities.

The Security Office performs a security audit. Typically, outside firms are engaged to perform independent security audits. These firms attempt to compromise JUSTIS and report on their findings. The results of the exercise are used to plan strengthening measures for the network infrastructure, data, applications, systems, and facilities.

[5] METAGroup Power Summit, Security: The Cornerstone of E-Commerce, June 18, 1999

The Security Office performs a security policy audit. The newly formed Security Office should collect and review all existing security policy statements from all agencies. The Security Office should assume the responsibility of organizing, publishing, managing and enforcing this enterprise-wide security policy.

The Security Office reviews and enhances security infrastructure elements. For example, Firewall policies and standards are an important element of a secure environment. The use of DHCP and non-routable internal IP addresses should also be reviewed to ensure that internal host addresses are hidden from external view through firewall re-mapping.

3.6.7 Operations Department

JUSTIS requires a well-trained operations staff for ongoing operations and administration of the system. Operations staff is critical to maintaining the functionality of the system by:

- Maintaining facilities personnel on a 24 by 7 basis.
- Maintaining disaster avoidance practices such as routine backups and preventive maintenance.
- Maintaining disaster recovery practices such as the development and exercise of a JUSTIS disaster recovery plan.
- Monitoring system use and maintaining log files.
- Monitoring system performance.
- Managing hardware and software licenses and maintenance contracts.

3.6.8 Help Desk Department

In order to take advantage of all the JUSTIS capabilities, it is recommended that users, once granted access, attend training. Also, once the user community becomes sufficiently large, as determined by the ITAC, a help desk will be needed to provide end-user support.

3.6.9 Applications Development Department

The applications development department will be comparatively large during phased JUSTIS implementation and will reduce in number as the system nears full implementation. A number of roles within this organization might be fulfilled by a single individual. These roles and their duties include:

Web Site Content Originator

The Content Originator creates content and maintains a fresh, valuable, quality electronic information product.

Web Site Content Owner

The Content Owners serve as the experts in a given content area. They have the responsibility of managing and providing updated information for a particular section of the site. The Content Owner is often the Content Originator but should always have review and approval authority.

Web Site Content Authority

The Content Authority approves and prioritizes content change requests. The Content Authority is an essential big picture gatekeeper role in the process and is the one most often overlooked.

Web Site Enterprise Authority

The JUSTIS Manager is the primary Enterprise Authority for JUSTIS. The JUSTIS Manager must approve all Internet content and Web sites.

Implementation Manager

The Implementation Manager assigns technical resources for changes to the Web site. After content is created and approved, the implementation process begins. Depending on the type of content and the work level of the technical team, different people with different skill sets may be required.

Implementer

Implementers prepare content for installation. Implementers include HTML programmers, graphics designers, script writers, and any other technically skilled individuals required to prepare content for installation on the site. They will coordinate with the Content Authority to ensure the original intent is translated accurately to the site.

Web Publisher

The Web Publisher operates and manages the Web hosts.

Web Application Developer

Web Application Developers create, test, debug and maintain Web programs, Java Servlets, Java Server Pages, Active Server Pages and COM Objects.

Database Developer

The database developer works with agency legacy applications database administrators to understand, document and connect to participating agency databases.

3.6.10 Applications Maintenance Department

The applications maintenance department will be comparatively small during phased JUSTIS implementation and will grow in number as the system nears full implementation. The roles and duties are in this department are the same as in applications development.

3.6.11 Security Administration Department

The security administrator is responsible for carrying out the polices and procedures set forth by the Security Officer. The Security Administrator:

- Maintains JUSTIS users by creating, deleting or modifying user accounts and access privileges.
- Liaises with security officers and administrators from JUSTIS agency participants.
- Assists with auditing and monitoring activities.
- Maintains security log file information.

4. Current Systems Summary

In order to implement JUSTIS with the functionality described in the previous section "Future JUSTIS User Community and System," it is necessary to recognize what Information Technology (IT) challenges may exist by developing a summary of the current systems operating within the justice agencies. During the POC, the JUSTIS implementation team developed a summary of the current agency IT environments by utilizing documentation and conducting interviews with ITAC members and selected justice agency personnel.

The ITLO provided the JUSTIS implementation team with documentation that represented proof-of-concept engagement requirements, administrative and technical infrastructure summaries and analyses of justice agency business processes and future plans. The table below summarizes the documentation provided.

Subsequently in Phase 2, the Justice Research and Statistics Association (JRSA) developed and Automated Reference Materials (ARM) database that will be made available via the public access functionality due to be deployed in the next phase of JUSTIS. This database will provide agencies the opportunity to update the data listed in the following tables.

Summary of CJCC provided documentation

Title	Description
Agency System/Project Chart	Contains information about all the Agencies – Agency code, System Code and System Name
Agency Desktop/Workstation Summary	Contains information Agencies Hardware and Software information
Agency Network Summary	Summary of Agencies' Network Information
JUSTIS POC Participants	Contains information about POC participants
JUSTIS Expectations and Participants	Information about the Participants Expectations
Deliverables	What needs to be delivered as Proof-of-concept
Governance and Structure	Information about hierarchy of different work group, their purpose and mission
CJCC ITAC	Contains information about Justice Agency Infrastructure Vision
Tracking Number Discussion	Tracking number importance and information about it
CJCC	Interagency Agreement on Information Technology

Title	Description
Draft on National Task Force, Tech and Criminal Justice Information	Report about NTF on Privacy, technology and Criminal Justice Information
Paradigms and Prototypes	Security policy considerations for Justice Agency Executives in DC
Privacy, Technology and Criminal Justice Information	Summary of Survey Findings
The National Consortium for Justice Information	About Information
Judicial Administration	Information about DOJ
Information about Data Access Service Improvements	Status Packet
Business Engineering	Recommendation Workflow and Business Engineering
Project OMNI	Business Engineering As -Is Process Document for MPD operational Processes
Comparisons of Definitions in Title 28 & found in State Laws	Table of Comparisons
Draft Legislation	CJIS Regulation, State Laws, Recommendation etc
District WAN Scheme	WAN Guidelines and Procedures
Interagency automated Data	A CD containing information about different agencies information systems
Justice Grant Administration	Scope of Work
Tracking Number Utilization	Information about Tracking Number Utilization
Privacy and Security support for DC	Criminal Justice information system Intranet
Preliminary Assessment of MPD Information System	Assessment about MPD Information System
Enforcement assistance Formula Grant Program	DC Strategy of Enforcement assistance Formula Grant Programs
Development of Strategic Investment Plan	Final Project Report
Information Technology Architecture Standards	Guide to Information Technology Architecture Standards

- During the POC, the ITLO provided the JUSTIS implementation team the opportunity to conduct interviews with each member of the ITAC and other selected agency personnel. These interviews were conducted in an effort to gain further detail of current interagency business processes, specific agency IT environment, and key member's JUSTIS "vision."

- At this time the JUSTIS implementation team also attended various ITAC work group meetings, namely the Technical Working Group and the Privacy & Security Working Group.

The summary of the current IT environments in each of the agencies will help in identifying the concerns and constraints for those who use, administer and manage these environments. The identification of the concerns and constraints are critical to the development of the roadmap that will define the steps necessary to achieve the future JUSTIS system. This section provides a high-level summary of the known current IT environment that were in place within each of the criminal justice agencies, at the completion of the POC. Although at the time of publication of the current Blueprint much of this information is dated, nevertheless it lays the foundation for defining future directions for JUSTIS. This section focuses on three primary areas:

- Security Infrastructure

- Network Infrastructure

- JUSTIS Agency Legacy Applications and Data

4.1 Security Infrastructure

A required functionality of JUSTIS is to allow access to criminal justice data. Accessing criminal justice data through a technical architecture such as that utilized in by JUSTIS requires an emphasis on security. This emphasis is addressed in JUSTIS deliverable number 1.1.2, JUSTIS Security Architecture. This deliverable describes the current JUSTIS security architecture deployed in JUSTIS Phase 2.

4.2 Network Infrastructure

The uniqueness of the relationship of justice agencies of the District of Columbia has lead to a complex web of interconnectivity. District of Columbia agencies are centered around the DC Wide Area Network (DC WAN), while Federal justice agencies have independent WANs. Although the Federal Agencies each have

independent WANs, they many also have connections to the DC WAN. The figure below shows the agency connections.[6]

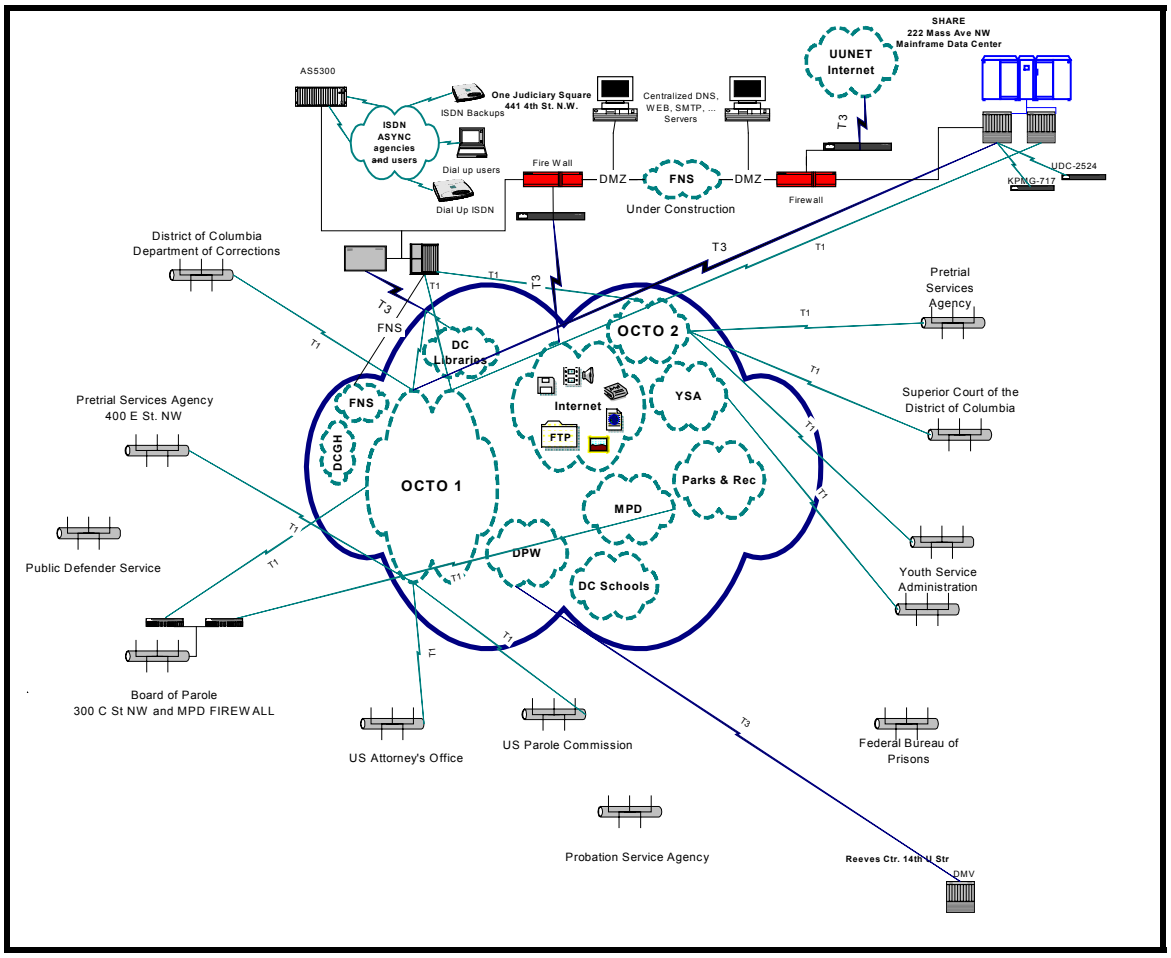


Figure 22 – Justice Agency Connection Points

[6] This diagram derived from the DC WAN diagrams provided by OCTO.

JUSTIS Agency Network Summary

Agency	DC WAN Connectivity	Network Topology	Network Hardware	Operating System	Protocols	WAN Services	Service Provider	Network Security	Maintenance
Office of the Chief Tech. Officer	6 SMDS Clouds, 464 Sites	Ethernet 10 Base – T Fast Ethernet	Cisco kentrox Digital Line	Novell NetWare 3.12-4.1 3 Servers MS NT Server 4.0 18 Server	TCP/IP IPX/SPX	9.6, 56K,T2, T3 ISDN	Bell Atlantic, UUNET	Cisco Pix 4.25	Internally Managed
Office of Corporation Counsel	T1 1 Site	Ethernet 10Base – T	Cisco Compaq	MS NT Server 4.0 10 Servers	TCP/IP Telnet	N/A	Bell Atlantic	MS Firewall Proxy 2.0	Internally Managed
CSOSA	T1 1 Site	Ethernet Fast Ethernet	Cisco	Novell NetWare 5.0 7 servers MS NT Server 4.0 20 Servers	TCP/IP IPX/SPX	Bell Atlantic Point to Point T1 fiber	UUNET	Secure Firewall Borderware	Internally Managed
DC Dept. of Correction	T1 25 Site	Ethernet Fast Ethernet	Cisco	20 Novell NetWare 4. 1 servers MS NT Server 4.0 5 Servers	TCP/IP IPX/SPX	Bell Atlantic T1	Bell Atlantic	Novell Firewall Border Messenger 3.0	Outsourced
DC Superior Court	T1 1 Site	Ethernet 10Base –T Fast Ethernet	Cisco Compaq Dell	Novell NetWare 4.0 1 Server MS NT Server 4.0 16 Server	TCP/IP IPX/SPX NetBEUI	Bell Atlantic T3	World Com MCI UUNET	Borderware	Internally Managed
Metropolitan Police Department	T1 25 Sites	Ethernet Fast Ethernet 10Base –T Gigabit Token Ring	Cisco 3Com	Novell NetWare 5.0 38 Servers MS NT Server 4.0 7 Servers Unix 6 servers	TCP/IP IPX/SPX	Bell Atlantic T1 9.6 56K	Digex	Checkpoint Firewall 4.0	Internally Managed
Public Defender	T1	Ethernet 10/100	Cisco	Windows NT Server 4.0	TCP/IP	Bell Atlantic T1 – 3	UUNET	MS Proxy 2.0	Internally Managed
US Attorney		Ethernet	Cisco	NT 4.0 Unix Servers	TCP/IP Telnet	Sprint ATM	Sprint	Raptor Firewall	Internally and Outsourced
US Parole Commission	T1		Cisco						
Youth Services Administration		TCP/IP	Cisco	MS NT Server 4.0 9 Servers		Bell Atlantic T1 and 56 K		Cisco Firewalls	

4.3 JUSTIS Legacy Applications and Data

This section provides a summary of the hardware, software, and database management systems in use by CJCC member agencies at the conclusion of the POC. This section also contains a high level summary of the data stored and managed in the information systems within the justice agencies.

The table below lists justice agency and their corresponding information system(s)[7].

JUSTIS Agency Legacy Application Summary

Agency	System Name	Description
Court Services & Offender Supervision	Automated Bail Agency Database	Defendant database with 250K + names with 12K active.
	Drug Test Management System (DTMS)	Totally automated & Paperless drug testing using barcode
	PRISM	To replace ABA DABA and DTMS
	CSOSA LAN	LAN Connects all CSOSA sites via T1
	Web Server	With dedicated Internet connection w/firewall
	Pretrial – Novel SAA Gateway	Connection to MPD Mainframe
	Probation – PARS	Probation, case workers assignments
	Parole – Parole Information System (PARIS)	Automated parole determination, decision -making
	Parole – Integration of new PARIS with PSA 's PRISM	Integrating the new PARIS with PSA's PRISM and MPD's
	Parole – Image parolee Case Folders	Using the Kodak's Imaging Business Solution software (IBS)
DC Department of Corrections	DOC WAN	16 LAN's with 20 Novell 4.11 Servers, 5 Windows NT4.0

[7] This list was completed prior to Y2K system evaluations and also does not reflect development of new systems and elimination of old systems eighteen months prior to August 31,2000. The CJCC currently has contracted a separate ongoing project with the JUSTIS Research and Statistics Association to update its agency information system records. Upon completion of the CJCC project, this chart will be updated accordingly

Agency	System Name	Description
DC Department or Corrections	CRISYS	Inmate records management system includes books
	JALAN	Inmate finance, commissary, and visitation
	New Jail Management System	New System will include CRISYS and JALAN functionality
	Integration with MPD's RMS	To integrate booking, demographics, mugshots, live scan.
	Other Integration Projects	Expected integration with contract facilities.
	Medical Logic	Medical records, appointments, inmate pharmacy
	KRONOS	Automated time and attendance
	HIEDI	Employee substance abuse monitoring
	Lotus Notes	Correspondence tracking, incident reporting and cost auditing
	JAACS	This system runs on a Lotus Web Server and provides access to the booking information along with mugshots.
Metropolitan Police Department	Washington Area Law Enforcement System(WALES)	State files & interface for NCIC, warrants, MPD, registration
	Criminal Justice Information System(CJIS)	Criminal history information
	Records Management System (RMS)	Records management, replacement for CJIS/WALES
	Automated Reporting System	Police reporting (UCS reporting software)
	Mobile Data Computers	Laptops in police vehicles

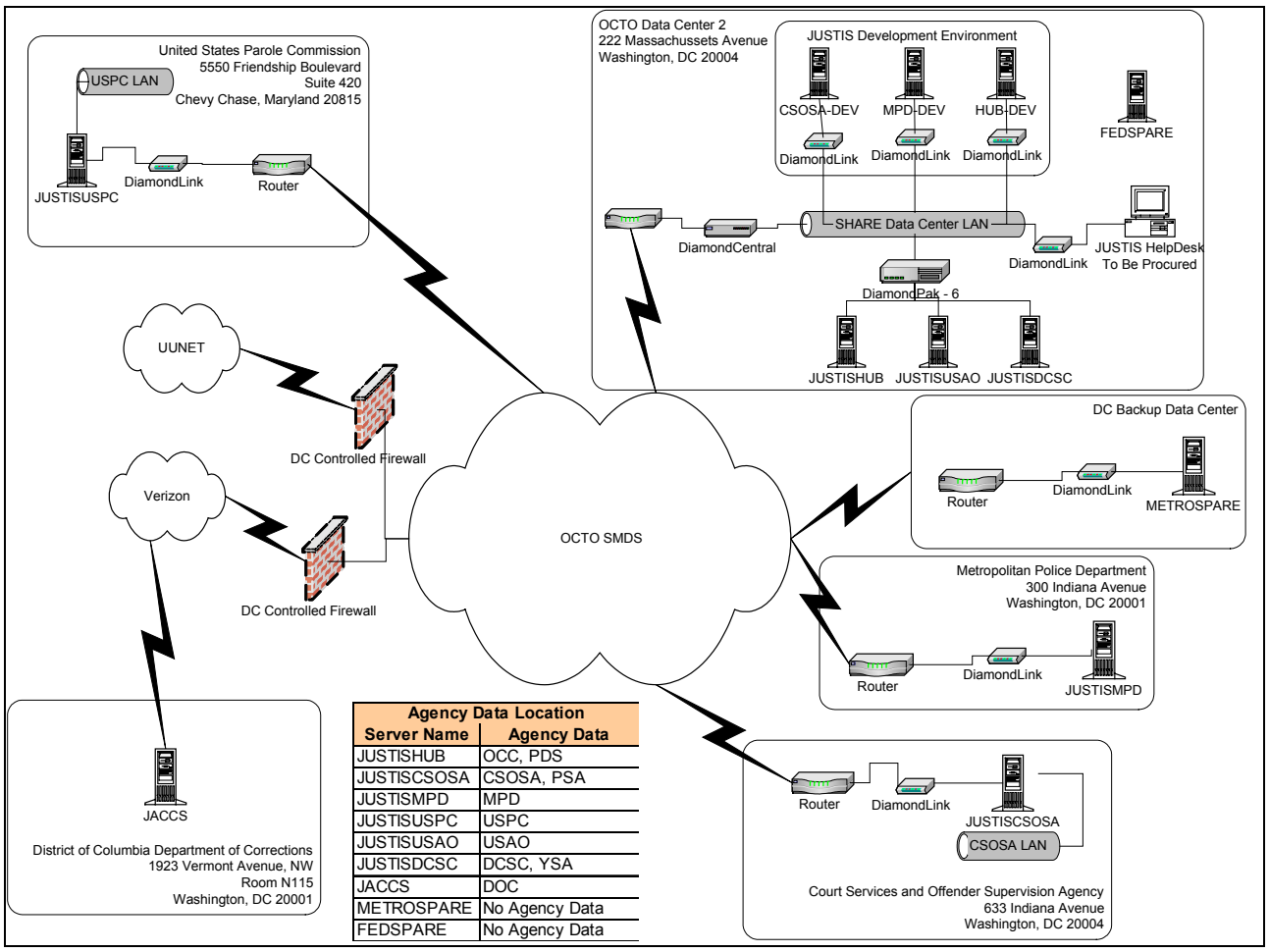
Agency	System Name	Description
Metropolitan Police Department	Message Switch	To handle NCIC communications and data exchanges
	MapInfo GIS	The central crime analysis unit at MPD headquarters
	ArcInfo & ArcView Geographic Information System (GIS)	Intranet map server, distributed capability for districts
	Washington Area Criminal Intelligence Information System	Investigative case management(Homicides, other cases
	Property Evidence Inventory Control System (PEICS)	Records on MPD seized property, contains CCN#s DEA#s
	Time & Attendance Court Information System (TACIS)	Automated capture of MPD employee's time and attendance
	Computer Assisted Dispatch (CAD)	Used for MPD dispatchers, contains a log of calls for service
	AFIS/Livescan	Fingerprint identification system. Mugshot storage system
	Full SUISS	Investigative case management system for all investigated
	FMS (R-Stars)	
	External Interface/Communications Strategy	To eliminate all dumb terminals for desktop applications
	MPDNet	MPD's internal network for desktop applications
	Internet Access	Access to DC WAN
	Desktops	All desktops upgraded to Pentium/NT
	Kiosks & Website	

Agency	System Name	Description
Office of Corporation Counsel	Case Management and Processing system	Home grown dBASE system currently used
	LAN	No LAN in place this time
Public Defender Services	Network	IBMS AS-400 token ring utilization MS Operating system
	Accounts Payable system	Home Grown System
	Personal System	Home Grown System
	Case Tracking Database System	Home Grown System and used for attorney statistics
DC Superior Court	DC Superior Court Mainframe	IBM ES9121-320, MVS-ESA, CICS, IDMS/R
	DC Superior Court LAN	10/100 Base T with CISCO routers, Bay networks hubs
	Connectivity to the Internet and the DCWAN	To have Internet access email, direct inter-agency gateways
	Web Page Development	DC Superior Court web Page
	Secure Firewalls	To limit access to authorized users
	Criminal Information System	Criminal Record maintenance system
	Juvenile Information System (JISRA)	1981-98 Juvenile records
	Transaction Data Management System (TDM)	Civil data maintenance system
	Domestic Relations Systems	Domestic relation case record system
	Jury Information System	Jury process application system
	Court Reporter Information System (CRP)	Contains court reporter data information
	Probate Data Information System (PRO)	Contains probate case information
	Personal Data System	Personal data record maintenance system

Agency	System Name	Description
DC Superior Court	Child Support Enforcement and Collections	N.O.I, IRS Intercept, wage attachment
	Courtwide caseload Management system	To replace current systems
	OPAL Middleware	Domestic Violence In-Take
	Juvenile Drug Court	To integrate JISRA/DTMS(PRISM)
	Legacy Systems	To make systems Y2K compliant
United States Attorney's Office	Network	USAO network with multiple servers, 486 and Pentium
	Replicated Criminal Information System (RCIS)	Imports CJIS, CIS data on daily basis into Oracle database
	Victim witness automated Transaction Statistics (VWATS)	Capture victim data at the time of intake
	Search warrant automated Transaction Statistics (SWATS)	Tracks search warrants issued in specific public addresses
	Personal Transaction Statistics (PTS)	Tracks personal, administrative information on employee
	Legal Information office network system(LIONS)	Tracks federal criminal and civil investigations and cases
Youth Services Administration	Adolescent Transaction Statistics (ACTS)	Maintains client records of basic, personal, family information
	Mini – Computer	IBM AS/400 mini computer that houses the ACTS

4.4 Current Network Design

The following diagram displays the current JUSTIS network layout developed during JUSTIS Phase 2. The diagram illustrates JUSTIS server placement and the current replicated data locations. The diagram will be continually updated to depict all new developments, as JUSTIS is continually deployed.



Agency Data Location	
Server Name	**Agency Data**
JUSTISHUB	OCC, PDS
JUSTISCSOSA	CSOSA, PSA
JUSTISMPD	MPD
JUSTISUSPC	USPC
JUSTISUSAO	USAO
JUSTISDCSC	DCSC, YSA
JACCS	DOC
METROSPARE	No Agency Data
FEDSPARE	No Agency Data

Figure 23 – JUSTIS Phase 2 Technical Architecture

4.5 User Workstations

The table below contains a summary of the current workstations at each of the justice agencies in the District of Columbia.[8]

Agency User Workstation Summary

Agency	Desktop Platforms	Operating System	Internet Browser	Internet Access	Virus Protection
Office of Corporation Counsel	350 – 300Mhz, PIII, 64 MB RAM 6GB HDD	350 – Windows NT	350 – IE, 5 - Netscape 4.0	20	McAfee 4.0.7
C.S.O.S.A	550Mhz PIII 128 MB RAM 8GB HDD ~800	Windows 98 ~750, NT4.0 ~50	IE ~800	~800	Norton AV ~800
DC Department of Correction	550Mhz PIII 128 MB RAM 12G HDD ~130	NT 4.0	IE5.0	35	McAfee 4.0.2
	500Mhz PIII 128MB RAM 10GB HDD ~50	NT 4.0	IE 5.0	40	McAfee 4.0.2
	450Mhz Pentium III 128 MB RAM, 10 GB HDD ~25	NT 4.0	IE 5.0	25	McAfee 4.0.2
	Pentium II 400Mhz 128MB RAM 2GBHDD ~150	Windows 95	IE 5.0	10	McAfee 4.02

[8] This will also be updated at the conclusion of the CJCC agency information system update project.

Agency	Desktop Platforms	Operating System	Internet Browser	Internet Access	Virus Protection
	266Mhz Pentium 64MB RAM 2GB HDD ~150	Windows 95	IE 5.0	50	McAfee 4.02
	133Mhz Pentium 16MB RAM 2GB HDD ~130	Windows 95	IE 5.0	65	McAfee 4.02
DC Superior Court	233–300Mhz 32-64 MB RAM 1.3 GB HDD ~500	W95/98 ~500	IE5.0 ~100	~100	Norton
Metropolitan Police Department	450Mhz PII 126MB 6GB ~1000	NT 4.0	Netscape	~1000	Norton
	450Mhz PII 126MB 6GB ~1000	NT 4.0	Netscape	~1000	Norton
	4500Mhz PII 128MB 9GB ~400	NT4.0	IE4.0	~400	Norton
	166-233Mhz 32-64MB 2GB ~350	NT4.0 W95/98	Netscape	~350	Norton
	266Mhz 64 MB 6GB ~100	NT4.0 W95/98	Netscape	~100	Norton
Public Defender	Micron Pent II 350Mhz 64 MB RAM 24XCD ROM 8GHD 3Com 10/100 NIC ~150	WidowsNT~50 Win 95 ~100	IE5.0 ~205	~205	Scan Mail for exchange server ~1 & Inoculate IT V4.53 Server & Workstation ~250

Agency	Desktop Platforms	Operating System	Internet Browser	Internet Access	Virus Protection
	Micron Pent III 400Mhz 64 MB RAM 8GHD 3Com 10/100 NIC ~40	Win 95	IE 5.0	40	Inoculate IT V4.53 Server & Workstation
	HP Vectra P100 24 MB RAM 2.5GHD 3Com 10/100 NIC ~15	Win 95	IE 5.0	15	Inoculate IT V4.53 Server & Workstation
US Attorney	366 MHZ Pentium 128 MB ~ 800	WinNT ~800	Netscape 4.7	~800	Inoculan 4.0 for NT ~800
US Parole Commission					
Youth Services Administration	350 Mhz PentIII 128 MB RAM ~115	Win NT ~115	IE5.0	~115	VirusScan 4.0

4.6 JUSTIS POC

This section discusses the infrastructure and operations that were in place at the conclusion of the POC on January 18, 2001. As stated in previous sections, the POC involved three agencies, MPD, PSA, and CSOSA. The central objective of the delivery of the POC was to provide the CJCC member agencies with a model of data sharing functionality, while adhering to the council's business requirements.

4.6.1 JUSTIS Infrastructure

The following diagram illustrates the network infrastructure that resulted from the implementation of the POC. The POC involved the installation of three primary servers and the creation of a Development Environment. Further details concerning the primary server configuration and location are included JUSTIS deliverable number 1.14, JUSTIS Hardware Expansion Plan.

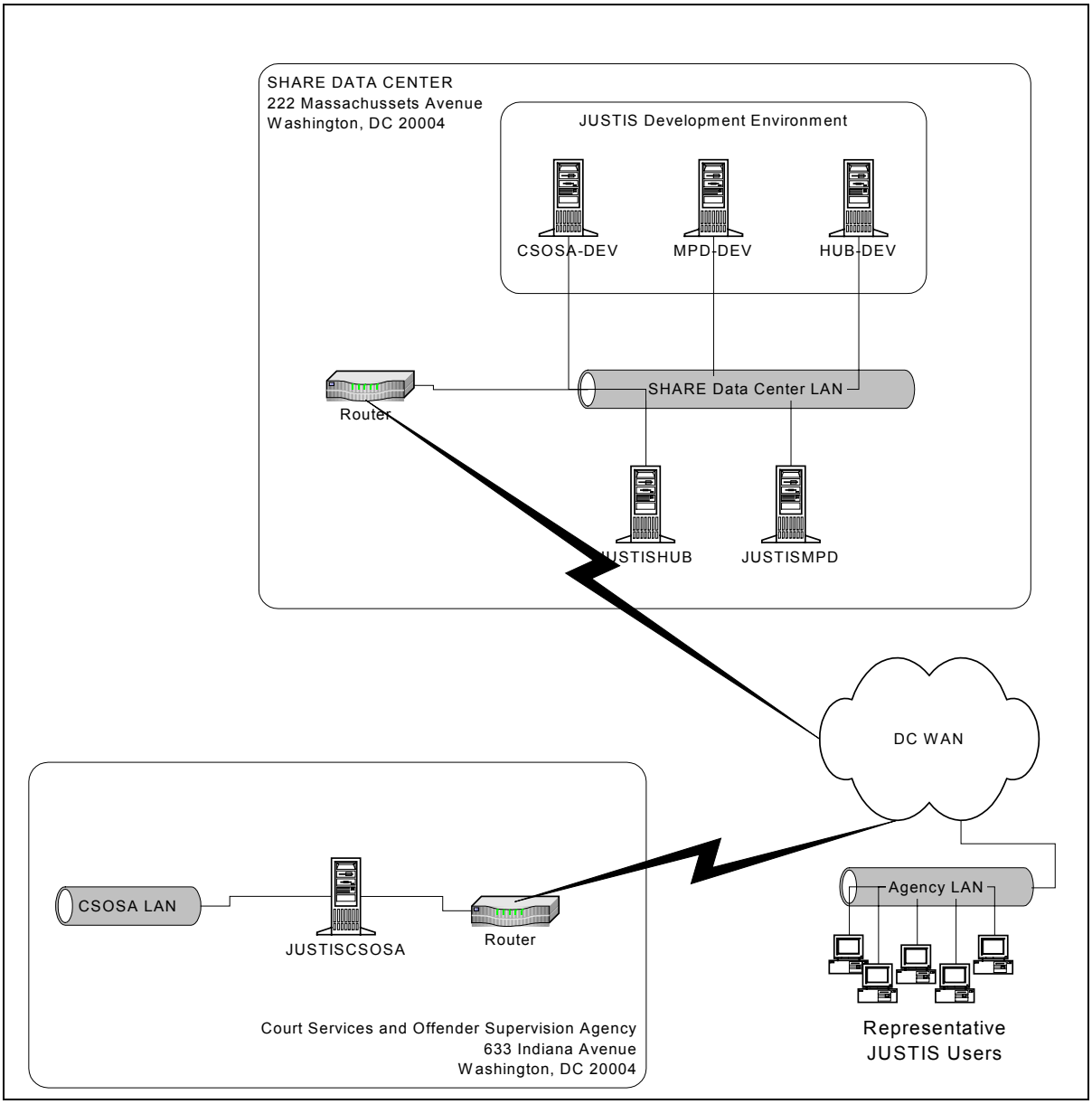


Figure 24 – JUSTIS POC Network Diagram

4.6.2 *POC Operations*

The POC data sharing functionality is enabled through three primary servers, JUSTISHUB, JUSTISMPD, and JUSTISCSOSA. The JUSTISHUB is the central facility, containing the JUSTIS applications and web interfaces. The two secondary servers contain the agency specific data. The JUSTISMPD server

maintains the corresponding MPD database, while the JUSTISCSOSA server maintains the databases for both CSOSA and PSA.

Data sharing functionality is established through the use of the JUSTIS Inquiry Application, located on the JUSTIS Hub server. This application has been developed as a broker between the user inquiry and the agency data. Based upon user inquiry, the application returns to the user what records are available and which particular agency has the records. The user then is able to select records for review. The inquiry application is able to retrieve the record from the particular agency and return the encrypted record to the user via the DC WAN. Please refer to the Future System section for a more detailed explanation of the data sharing functionality.

4.7 JUSTIS Phase 2

This section describes the expanded JUSTIS infrastructure as illustrated in Figure 23. This infrastructure built upon the existing POC infrastructure by adding servers to support the data contribution expansion as outlined in the Phase 2 statement of work.

4.7.1 JUSTIS Infrastructure

JUSTIS Phase 2 Infrastructure maintains the same conceptual framework deployed in the POC. The JUSTISHUB server remains the central facility to which all agency servers connect. The primary difference between the POC and Phase 2 infrastructure is the addition of the JUSTISUSAO, JUSTISUSPC, JUSTISDCSC, FEDSPARE, and METROSPARE servers. Also incorporated with the implementation of Phase 2 is the direct Internet connection to the Jail and Community Corrections System (JACCS) maintained by the District of Columbia Department of Corrections (DCDC).

4.7.2 Phase 2 Operations

Although significant hardware expansion is incorporated with the implementation of Phase 2, the operation of JUSTIS remains the same. Figure 23 illustrates the where the replicated data is stored. The JUSTISHUB will access the additional databases located on the servers and continue to provide a unified view to the JUSTIS users.

4.8 Summary

The information presented above provides a summary of the current IT environments within the justice agencies, and a brief description of the JUSTIS network environment that resulted from the implementation of the POC and JUSTIS Phase 2. This information will be compared with the IT infrastructure requirements set forth in the Future Systems section of the JUSTIS Blueprint. This comparison generates a list of “gap” points that are laid out in the next section of the document. These “gap” points provide the basis for the development of the roadmap, which will present a logical process for a multi-phased implementation of JUSTIS.

It is worth noting that CJCC member agencies and OCTO are constantly working to enhance their information systems and the corresponding infrastructures. Therefore, the data presented here is only as accurate as the data available at time of publication. Moreover, the deployment of the ARM database will provide the facility that will shorten the lag time between agency information system improvement and CJCC recognition and documentation of the improvement. The ARM will provide the developers of the Blueprint a resource that will support the Blueprint update effort. The support provided will ensure the data contained in this section will be relatively up-to-date.

5. Roadmap

5.1 Introduction

This Blueprint document began with a definition of the system's mission and business requirements. It then moved on to a description of the complete vision for the future JUSTIS system once it has been fully developed and implemented. Those sections collectively define the end-state goal.

The preceding section summarized the elements of the current environment. That section defines the current point from which JUSTIS and its community of users must start towards the eventual end-state goal.

This section presents an analysis of the gap areas between where we are and where we want to be. Once these gap areas are identified, organized and prioritized, a roadmap is presented. This roadmap shows a number of steps towards the full implementation. The following diagram depicts how we have proceeded through this document, and we are now in the final steps:

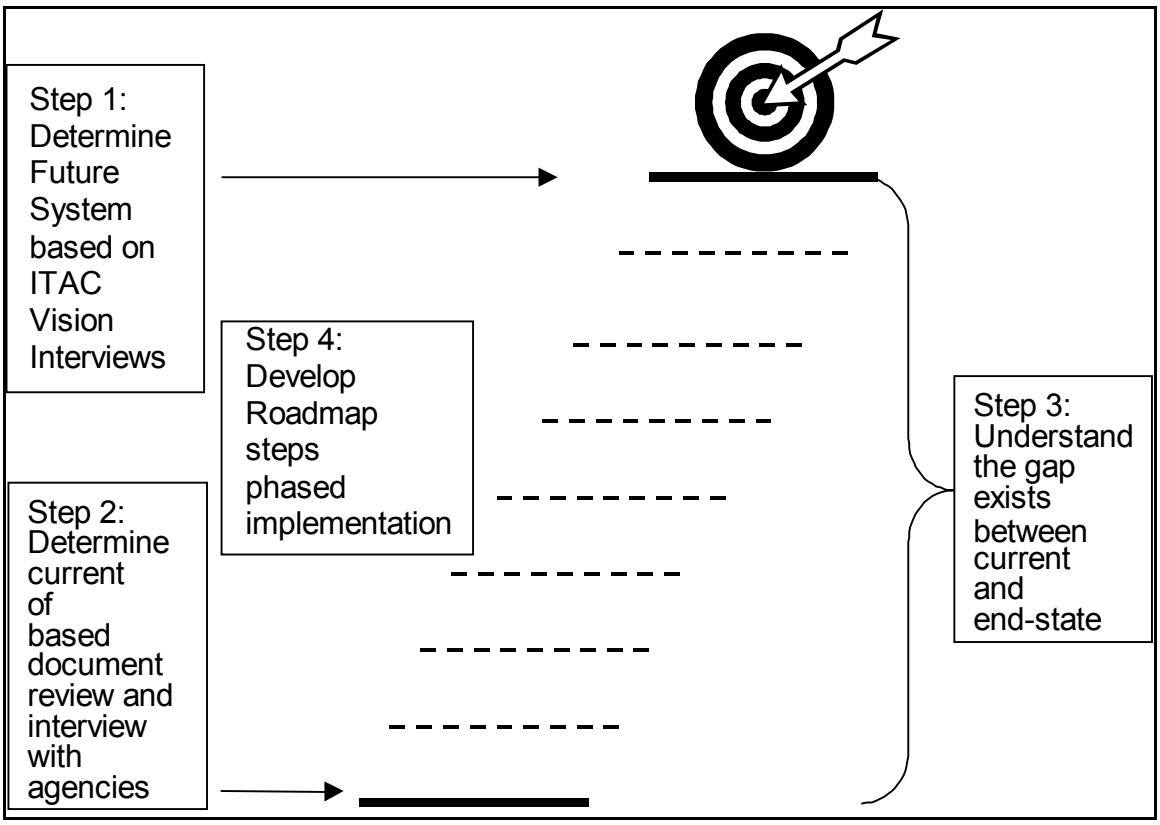


Figure 25 – Blueprint Format

JUSTIS will be implemented in phases. This allows the justice user community to realize short-term gains while proceeding toward the entire vision. Multi-phase implementation also allows the system to keep in time with contemporary technologies throughout the implementation. The roadmap defines the phased implementation.

5.2 Identification of Gap Areas

The variance between current environment capabilities vis-à-vis the environment necessary to support the full JUSTIS system is analyzed in this section. Initially, JUSTIS was a relatively new system for the District of Columbia and the gaps were substantial. Over the past year, with the implementation of both the POC and Phase 2 the gaps have been significantly closed.

5.2.1 Gap Areas for the Functional Requirements

5.2.1.1 Agency Participation and Information Sharing Modes

At the conclusion of the proof-of-concept phase, three agencies were participating by contributing their data. These are the Metropolitan Police Department, Pretrial Services Agency and Court Services and Offender Supervision Agency. Additionally, five agencies participated with three users each to evaluate the proof-of-concept system.

During JUSTIS Phase 2, the agency participation was expanded to included ten of the eleven CJCC member agencies. All member agencies with the exception of the Bureau of Prisons (BOP) participated in the contribution of public safety data to JUSTIS. Also, the participating agencies were provided the opportunity to obtain user access to JUSTIS for their respective agency employees.

As a result of the successful implementation of JUSTIS, agencies outside of the CJCC have requested access and the ability to contribute data. This will build upon the agency expansion accomplished in Phase 2. During future phases, JUSTIS will invite the United Sates Marshal Service (USMS) to have access only, the Federal Public Defender (FPD) to become a contributor and to have access, the United States District Court (USDC) to become a contributor and to have access, the Federal Bureau of Prisons (BOP) to have access only, and the Department of Motor Vehicles (DMV) to become contributor only.

This desire for expansion has created a new gap. Therefore this gap is to expand the agency data contributors to include those referenced above and to increase the number of individual users of the system. Currently this gap is to be addressed in JUSTIS Phase 3.

5.2.1.2 Notification Services: Publish and Subscribe

Under both the POC and Phase 2, notification services were not scheduled for implementation. This functionality has been initially scheduled for development and deployment in Phase 3. The gap here remains and is to be initiated with the implementation of the JAD sessions as described in the future system description

5.2.1.3 Collaborative Services: Discussion Groups

Discussion groups as defined by the Blueprint are not yet part of JUSTIS. The gap remains the definition development of the requirements of the system, the selection and purchase of software that meets those requirements, the implementation of the software and finally the complete implementation of a robust discussion group system and the following system administration.

5.2.1.4 Data Transfer

Data transfer was not scheduled for implementation during Phase 2. To close this gap, the initiation of data transfer JAD session must take place. The session participants will need to identify likely areas for data exchange, analyze mechanisms available to enable limited data exchange (such as file transfers or manual disk exchange) and work with the all agencies to design programs and procedures to enable JUSTIS data transfer.

5.2.1.5 Data Quality Alliance

Data cleansing and notification processes are currently not developed or implemented as part of JUSTIS. Initiating JAD sessions with all agency stakeholders involved. This will initiate the design process and conclude with a deployment. A conceptual design is described in the Future User Community and System section of this document.

5.2.1.6 Public Access

Public access has been partially satisfied through the development of the CJCCDC.org website. Continuing the tangible value brought to the public via JUSTIS, the CJCCDC.org website must provide access to other commonly requested public data. This gap remains. Fulfilling this gap will require the migration of the CJCCDC.org website to include links to other websites that contain publicly accessible public safety data and the development of additional applications that provide data that is not currently readily available.

5.2.1.7 Statistical Analysis Center

A complete statistical analysis center goes beyond the scope JUSTIS and to implement such a center would violate one of the solutions primary business requirements. The need to modify agency systems would place constraints and requirements upon participating agency data systems. Although the development of a complete system would violate a business requirement, the development of the foundation required would not. Therefore, the development of a Statistical Analysis Center can be initiated through JUSTIS. This defines the gap and closing of the gap would require the guidance of a District of Columbia Statistical Analysis Center Director. The Director would initiate JAD sessions with select agencies. The design and development would follow the JAD sessions.

5.2.2 Gap Areas for the Technical Architecture

The gap areas between the current technical architecture and the architecture necessary to support JUSTIS are as follows:

- **Full security implementation**. The requirements and the subsequent technical architecture needs are outlined in the JUSTIS Phase 2 deliverable number 1.1.2, JUSTIS Security Architecture. This document concludes with a proposed solution that is an enhancement upon the current security architecture deployment. New functionality implemented with JUSTIS will require this security implementation to be revisited. Also an enhance PKI deployment to the users is recommended.

- **JUSTIS building blocks**. The continued use of Microsoft Development standards will continue throughout JUSTIS. New releases in the standards will require evaluation in future JUSTIS phases.

- **Physical Plant Design.** The JUSTIS POC began with a physical plant design that will be compatible with the final version of JUSTIS. The District will need to evaluate machine room locations for further JUSTIS expansion. Any expansion should be considerate of the scenarios outlined in the JUSTIS deliverable number 1.4, JUSTIS Hardware Expansion Plan

- **Scalability and Performance Requirements.** The performance should be monitored by the JUSTIS operations staff and performance evaluation should be made in accordance with JUSTIS deliverables 1.4 and 1.5, the JUSTIS Software Upgrade Plan and JUSTIS Hardware Expansion Plan, respectively.

- **User workstations.** All user workstations should be able to run a modern web browser such as Microsoft Internet Explorer or Netscape. JUSTIS participating

agencies should review their user workstations in relation to this requirement. Older terminals, such as IBM 3270 devices, should be scheduled for upgrade.

- **Network Infrastructure: special security requirements.** Security is a continual concern. Currently the network security requirements have been identified in JUSTIS deliverables 1.1.2, the JUSTIS Security Architecture, and 1.7, the JUSTIS Security Policy and Procedures. As the JUSTIS is expanded and as participating agencies modify their infrastructures, these documents need to revisit for update.

- **Off-line, Replicated and On-line Data**. As agencies are added to the JUSTIS community, each will need to decide the strategy for making their data available to the participants. The methodologies employed by the current participating agencies are documented in JUSTIS deliverable 4.1, JUSTIS Data Contribution Design Documents. The incorporation of any additional agencies or the modification of any current agencies will require this deliverable to be updated.

5.2.3 *Gap Areas for Management and Administrative Structure*

The future administrative and management structure for JUSTIS was defined as follows:

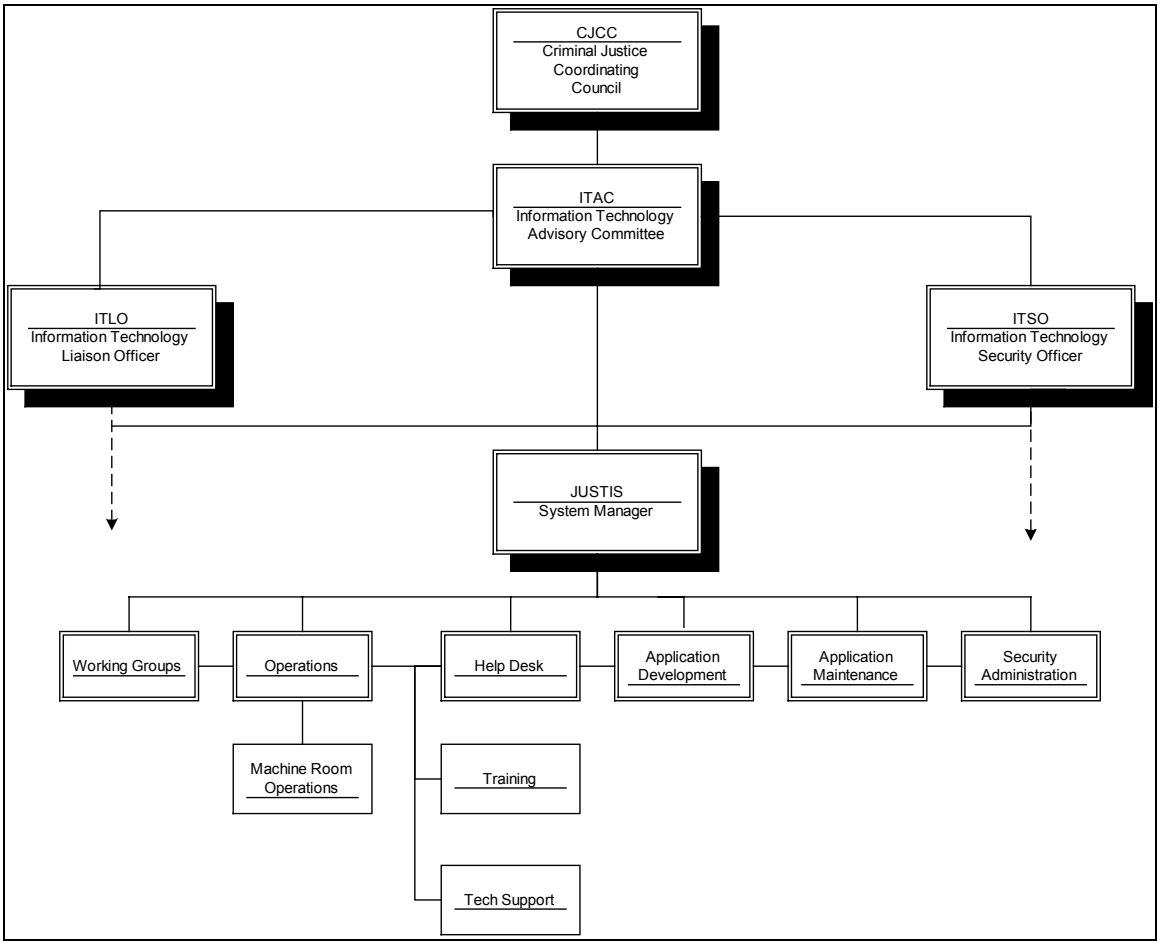


Figure 26 – Future JUSTIS Administrative and Management Structure

JUSTIS is being implemented in phases, and the JUSTIS office structure will also be implemented in phases. During the proof-of-concept phase, the JUSTIS team was organized as follows:

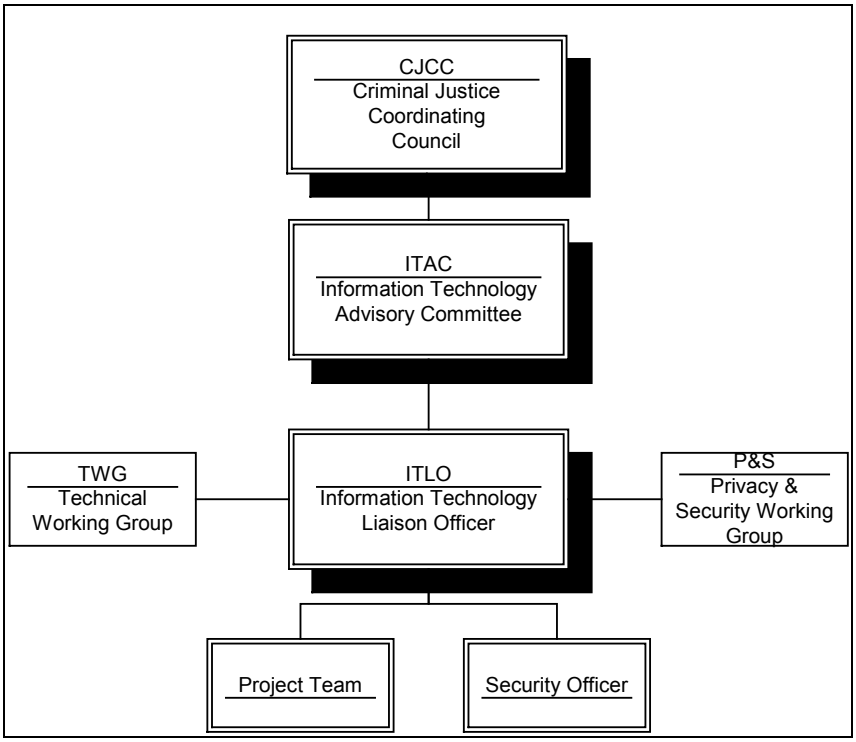


Figure 27 – POC JUSTIS Administrative and Management Structure

In this structure, the project team was from KPMG Consulting, Inc. and performed a subset of the duties that ultimately spread across Operations, Help Desk, Applications Development and Application Maintenance. The project team is received guidance from the Technical Working Group during POC development. The project team was managed by the ITLO.

CJCC staff fulfilled the Information Technology Security Officer role with supplemental assistance from Mitretek. The security team received guidance from the Privacy and Security Working Group during POC development.

Once the POC had been developed and deployed, the JUSTIS office structure changed slightly for Phase 2. This change was to accommodate an environment where the current system needs support and at the same time system functionality is being enhanced. This transition structure is depicted in the following diagram:

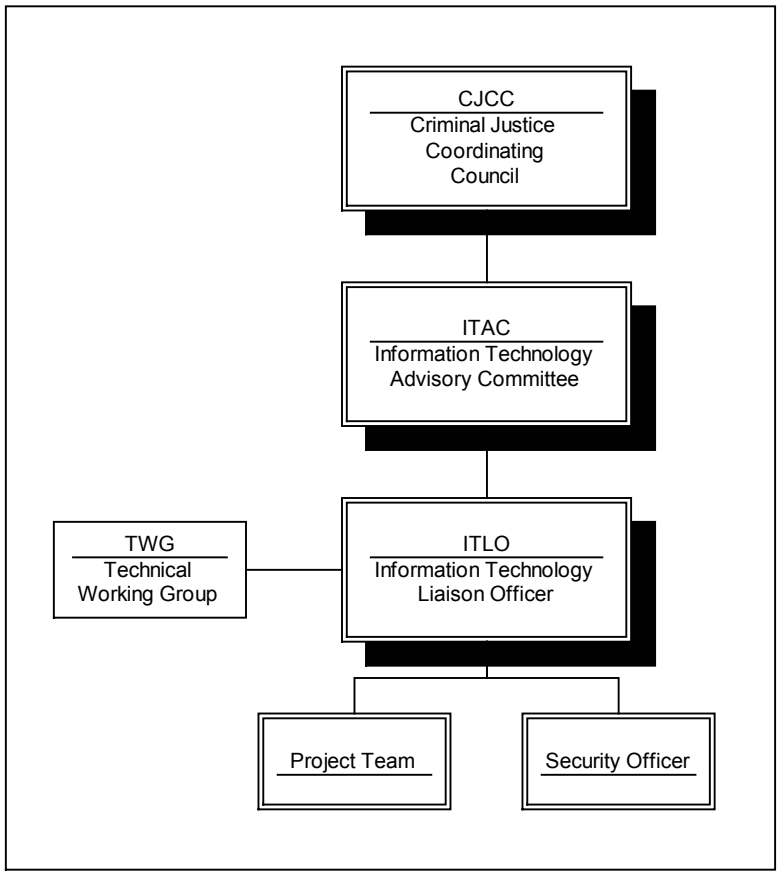


Figure 28 – Phase 2 JUSTIS Administrative and Management Structure

Upon completion of Phase 2, the JUSTIS office structure was modified again, to accommodate the increase number of users, the increased data contribution, to manage the security infrastructure, and to support continued development of need functionality. This transitive structure is depicted in the following diagram:

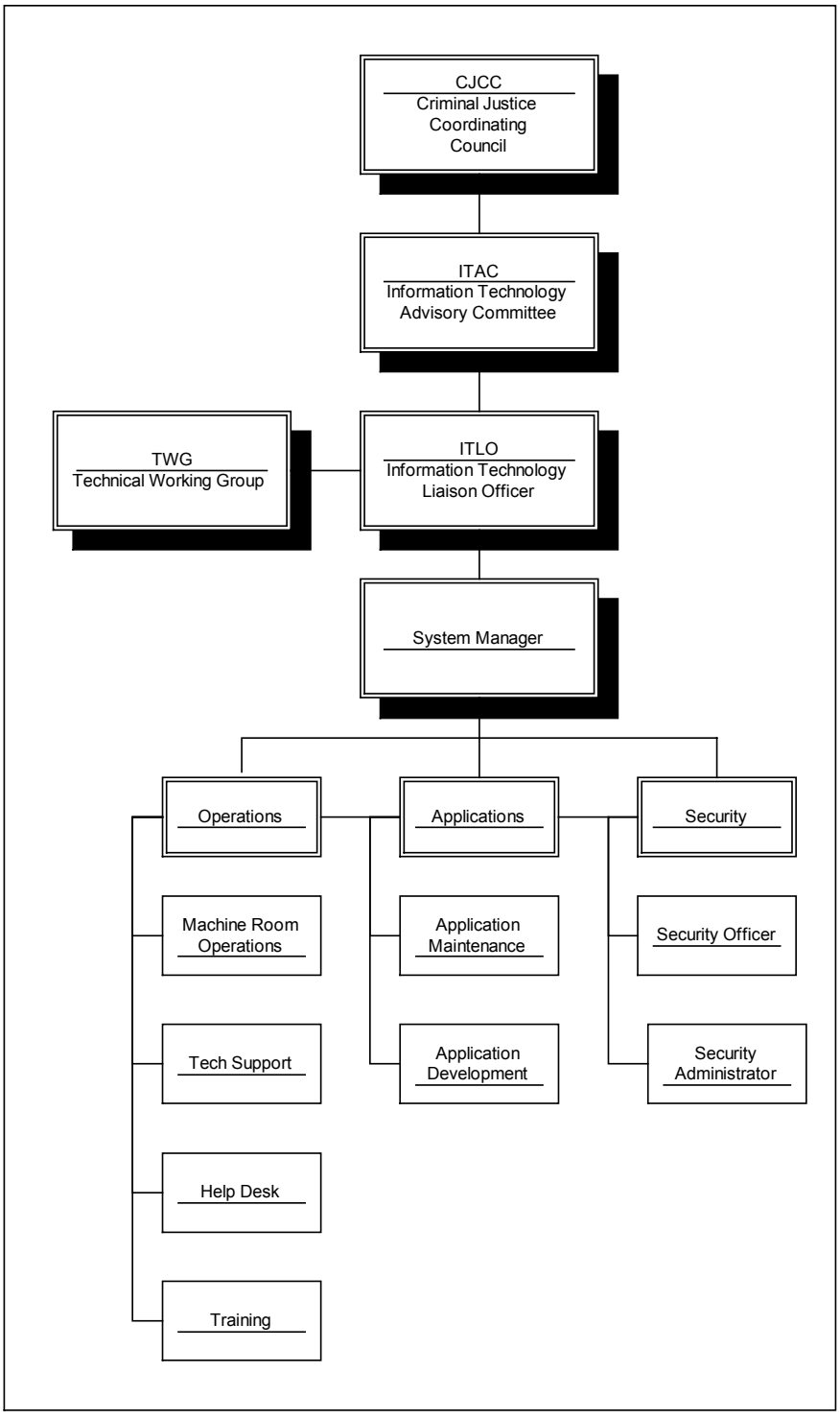


Figure 29 – Interim JUSTIS Administrative and Management Structure

The above diagram depicts a separation of departmental roles and each staff box **does not necessarily represent a single staff member**. During this transition stage, some staff overlap occurred. For example, in the help desk department, a single staff member also handled some training and operations duties. During this phase, applications maintenance was the responsibility of the application development staff.

Once in production, management of the system is the leading contributor to the system's effectiveness. The complexity of the relationships of the justice agencies in the District of Columbia necessitates an independent management and administrative office for the JUSTIS. A major function of this office is to formulate the correct rules of publication and access to criminal justice data.

5.3 Summary and Prioritization Ranking of Gap Areas

The gap areas identified in the preceding section are organized in the table below. The organization is based in priority of implementation as well as interdependencies. An example of interdependency is that a security certificate server and infrastructure are necessary before secure electronic mail can be implemented. For completeness, the proof-of-concept and Phase 2 statement of work tasks are shown.

Summary and Prioritization Ranking of Gap Areas	
Create A JUSTIS Proof-Of-Concept	
	Perform initial review of existing DC produced work products.
	Identify and assign District "core" team members and justice agency representatives.
	Refine all project tasks as necessary.
	Finalize proof-of-concept project plan as required.
	Institute project record keeping and accounting procedures.
	Develop regular status meeting schedule.
	Establish project level communications plan, including CJCC, OCTO, ITAC and its sub-groups (e.g., Analysis and Design, Technical Work Group).
	Prepare proof-of-concept kick-off presentation materials.
	Conduct proof-of-concept kick-off meeting.
	Develop a Blueprint outline.
	Obtain approval of Blueprint outline.

Summary and Prioritization Ranking of Gap Areas	
	Obtain current technical architecture inputs from participating agencies (e.g., hardware/software inventories, architecture diagrams).
	Develop Blueprint working draft content.
	Conduct Blueprint walkthrough.
	Prepare Blueprint for distribution.
	Update Blueprint working draft.
	Distribute final Blueprint.
	Develop mock-up of a proposed framework.
	Obtain input from participating agencies for static content.
	Develop agency-specific static content.
	Develop general static content.
	Test web site components and links.
	Work with participating agencies to determine data to be published.
	Design screen formats.
	Design programs to access agency databases.
	Develop programs to access agency databases.
	Perform testing.
	Deploy application
	Develop requirements for the development environment.
	Support the acquisition of hardware/software/network components for the development environment.
	Support the set-up of the development environment.
	Development requirements for production environment.
	Support the acquisition of hardware/software/network components for the production environment.
	Support the set-up of the production environment.
	Document development and production environments
	Review adequacy of user workstations.
	Identify any needed upgrades.

Summary and Prioritization Ranking of Gap Areas	
	Prepare user workstations for implementation.
	Deploy browser and other appropriate software on three (3) workstations within five (5) agencies.
	Provide up to three (3) half-day training sessions to designated users or trainers.
	Deploy application to three (3) workstations within five (5) agencies.
	Document standard workstation configuration
Create a production environment for JUSTIS	
	Install production security hardware
	Install Discussion Group Software
	Install Certificate Authority server
	Implement security policies and procedures for JUSTIS users
	Implement system monitoring facilities
	Develop disaster recovery plan
	Develop operations procedures (backup/restore, preventive maintenance)
	Develop help desk materials – frequently asked questions, user manual
Increase Data Contribution	
	Superior Court of DC Data Contribution
	DC Department of Corrections Data Contribution
	US Parole Commission Data Contribution
	US Attorneys Office Data Contribution
	Youth Services Administration Data Contribution
	Office of Corporation Counsel Data Contribution
	Department of Motor Vehicles Data Contribution
	Federal Public Defender Data Contribution
	United States District Court Data Contribution
Prepare JUSTIS Agency Environment	
	Public Defender Service JUSTIS Server hardware and software
	DC Superior Court JUSTIS Server hardware and software

Summary and Prioritization Ranking of Gap Areas	
	DC Department of Corrections JUSTIS Server hardware and software
	US Parole Commission JUSTIS Server hardware and software
	US Attorneys Office JUSTIS Server hardware and software
	Youth Services Administration JUSTIS Server hardware and software
	Office of Corporation Counsel JUSTIS Server hardware and software
	Department of Motor Vehicles JUSTIS Server hardware and software
	Federal Public Defender JUSTIS Server hardware and software
	United States District Court JUSTIS Server hardware and software
	DC Department of Corrections provide static web content
	US Parole Commission provide static web content
	US Attorneys Office provide static web content
	Youth Services Administration provide static web content
	Office of Corporation Counsel provide static web content
	Federal Public Defender provide static web content
	Department of Motor Vehicles provide static web content
	United States District Court provide static web content
Prepare JUSTIS Users	
	Public Defender Service – identify JUSTIS users
	Superior Court of DC – identify JUSTIS users
	DC Department of Corrections – identify JUSTIS users
	US Parole Commission – identify JUSTIS users
	Federal Bureau of Prisons – identify JUSTIS users
	US Attorneys Office – identify JUSTIS users
	Youth Services Administration – identify JUSTIS users
	Office of Corporation Counsel – identify JUSTIS users
	Superior Court of DC – prepare user workstations
	DC Department of Corrections – prepare user workstations
	US Parole Commission – prepare user workstations

Summary and Prioritization Ranking of Gap Areas	
	US Attorneys Office – prepare user workstations
	Youth Services Administration – prepare user workstations
	Office of Corporation Counsel – prepare user workstations
	United States Marshal Service– prepare user workstations
	Federal Bureau of Prisons – prepare user workstations
	Federal Public Defender – prepare user workstations
	United States District Court – prepare user workstations
Increase JUSTIS Functionality	
	Enhance Security Features
	Setup discussion groups (e.g. assign moderator)
	Implement underlying messaging structure for notification
	Implement publish/subscribe event notification at group level
	Implement publish/subscribe event notification at individual level
	Implement infrastructure for statistical database
	Populate a statistical analysis database
	Develop statistical analysis queries
	Enhance CJCCDC.org website to provide controlled public access
	Analyze agencies for data transfer implementation needs
	Design interagency data transfer programs and procedures
	Test data transfer capabilities
	Fully implement and support data transfer

5.4 Proposed Phases of Implementation

Now that the gap items have been prioritized and analyzed for interdependencies, the gap items will be partitioned into phases for future release implementations of JUSTIS. In addition to priority and interdependence, phase steps have been chosen for their simplicity of implementation relative to the value they provide. This means

that early phases will combine items necessary for infrastructure support as well as items that return high value for a relatively small investment.

5.4.1 *Phase 1 – POC*

The POC solution has been defined and accepted in the original JUSTIS statement of work and the project plan approved by the ITAC on July 20, 2000. The POC demonstrated progress towards the future state by closing a number of gap items. The POC was the first step in a phased implementation of the full JUSTIS system. Future phases expand upon the core functionality initially deployed in the POC.

5.4.2 *Phase 2 – From POC to Production, Expand JUSTIS User Population, Increase Data Contribution*

Upon the completion of the POC the decision was made to move forward with a more complete JUSTIS implementation, the next step migrated the POC system to a production system within DC. This phase included increasing the numbers of users both within the POC participating agencies as well as with new agencies. Also in this phase required increased data contribution and the deployment of a security infrastructure.

Phase 2 Tasks	
Create a production environment for JUSTIS	
	Install production security hardware
	Implement security policies and procedures for JUSTIS users
	Implement system monitoring facilities
	Develop disaster recovery plan
	Develop operations procedures (backup/restore, preventive maintenance)
	Develop help desk materials – frequently asked questions, user manual
Prepare JUSTIS Users	
	Public Defender Services Agency – identify users
	Superior Court of DC – identify JUSTIS users
	DC Department of Corrections – identify JUSTIS users

Phase 2 Tasks	
	US Parole Commission – identify JUSTIS users
	US Attorneys Office – identify JUSTIS users
	Youth Services Administration – identify JUSTIS users
	Office of Corporation Counsel – identify JUSTIS users
Increase Data Contribution	
	Public Defender Service Data Contribution
	Superior Court of DC Data Contribution
	DC Department of Corrections Data Contribution
	US Parole Commission Data Contribution
	US Attorneys Office Data Contribution
	Youth Services Administration Data Contribution
	Office of Corporation Counsel Data Contribution
Prepare JUSTIS Agency Environment	
	Public Defender Service JUSTIS Server hardware and software
	DC Superior Court JUSTIS Server hardware and software
	DC Department of Corrections JUSTIS Server hardware and software
	US Parole Commission JUSTIS Server hardware and software
	US Attorneys Office JUSTIS Server hardware and software
	Youth Services Administration JUSTIS Server hardware and software
	Office of Corporation Counsel JUSTIS Server hardware and software
	Public Defender Service provide static web content
	DC Superior Court provide static web content
	DC Department of Corrections provide static web content
	US Parole Commission provide static web content
	US Attorneys Office provide static web content
	Youth Services Administration provide static web content
	Office of Corporation Counsel provide static web content

5.4.3 *Phase 3 – Enhance JUSTIS Functionality and Expand Agency Users and Contributors*

During this phase JUSTIS functionality is enhanced with the implementation of notification systems, core data transfer, the development of the data quality alliance, the enhancement of the public access functionality and the establishment of the Statistical Analysis Center. Agency users and contributors are also expanded in the phases to include agencies outside of the CJCC membership.

Phase 3 Tasks	
Increase JUSTIS Functionality	
	Enhance Security Features
	Setup discussion groups (e.g. assign moderator)
	Implement underlying messaging structure for notification
	Implement publish/subscribe event notification at group level
	Implement publish/subscribe event notification at individual level
	Implement infrastructure for statistical database
	Populate a statistical analysis database
	Develop statistical analysis queries
	Enhance CJCCDC.org website to provide controlled public access
	Analyze agencies for data transfer implementation needs
	Design interagency data transfer programs and procedures
	Test data transfer capabilities
Increase Data Contribution	
	Department of Motor Vehicles Data Contribution
	Federal Public Defender Data Contribution
	United States District Court Data Contribution
Prepare JUSTIS Agency Environment	
	Department of Motor Vehicles JUSTIS Server hardware and software
	Federal Public Defender JUSTIS Server hardware and software

Phase 3 Tasks	
	United States District Court JUSTIS Server hardware and software
	Federal Public Defender provide static web content
	Department of Motor Vehicles provide static web content
	United States District Court provide static web content
Prepare JUSTIS Users	
	United States Marshal Service– prepare user workstations
	Federal Bureau of Prisons – prepare user workstations
	Federal Public Defender – prepare user workstations
	United States District Court – prepare user workstations

6. Conclusion

6.1 JUSTIS Development and Implementation

The JUSTIS Proof of Concept as defined in the original statement of work was the first step in a phased implementation of the full JUSTIS system. It was during this phase, limited data sharing through the use of an inquiry application was accomplished. The success of the POC was due in large by the coordination of the three POC JUSTIS agencies (MPD, PSA, and CSOSA) and the assistance of OCTO which allowed the hosting of JUSTIS on the District of Columbia's Wide Area Network. The hardware and software configuration of JUSTIS is outlined in two Phase 2 deliverables numbered 1.4 and 1.5. The development team worked over the six months developing, implementing and coordinating this effort.

Following the POC a second phase was initiated by the CJCC. The objective of this phase was to increase data contribution by including the remaining outstanding CJCC agencies, automate the data contribution of all agencies, and to increase JUSTIS user community through the support and training of agency Information Technology Security Officers (ITSO).

The information system that resulted from the POC and Phase 2 is operational and currently the development team is maintaining JUSTIS as an operational system where the focus has been to ensure the production capabilities of JUSTIS, monitor the system, maintain the help desk, and maintain the web presentation of JUSTIS.

The implementation team is preparing for the initiation of a third phase to JUSTIS that will include the development of increased JUSTIS functionality and the increase of data contributing agencies to those outside of the CJCC. The expected functionality will include the foundations of notification systems, the beginnings of data transfer capabilities, a more robust data quality assurance process, and the enhancement of the current CJCCDC.org website.

6.2 Blueprint Architecture

The JUSTIS Blueprint is the foundation document of JUSTIS. This document was produced with the intention of describing and detailing the development of a solution that will serve the data sharing and collaboration needs of the CJCC participating agencies. JUSTIS is to become the backbone system servicing these needs. The JUSTIS Blueprint addresses the development of this System by focusing on the following critical implementation points:

- **The JUSTIS Business Requirements and Goals.** These requirements and goals were developed and managed by the CJCC for the benefit of the justice community

of the District of Columbia and are to be used as a continual reference points throughout the development of JUSTIS. They are to become the guidelines in the development of a Public Safety Community of Interest (COIN) within the District of Columbia and are dynamic enough to change as the COIN's environment changes.

- **The JUSTIS Implementation Strategy.** Implementation strategy is key in the development of highly technical information system. JUSTIS is designed with a multi-phased implementation strategy. This strategy provides advantages over a large, full-scale implementation. Short-term successes or quick wins are realized in an implementation strategy of this sort. Also, strategies such as this allow for the integration of current technologies throughout the implementation. Most importantly, a multi-phased implementation strategy provides time for validation of the long-term plan after each implementation phase.

- **The Future JUSTIS User Community and System.** The JUSTIS user community is made up of public safety agencies with the need for various elements of criminal justice data. These agencies also hold stores of criminal justice data that if transported securely, could be shared with other public safety agencies. The future JUSTIS system is designed to become a conduit in public safety agency data sharing and is described in its agreed upon "to be" form at the time of publication. Interagency functionalities of JUSTIS are centered on the JUSTIS business requirements and goals and implemented using the current technologies to date that correspond with those requirements and goals. The implementation of the desired interagency functionalities demands the integration of various technical architecture requirements. The JUSTIS technical architecture takes into account these architecture requirements and integrates them into a single architecture that considers system security, scalability, user workstations, network infrastructure, and application development along with other related factors.

- **The JUSTIS Community Current Systems Summary.** Becoming aware of the information technology environments residing in the public safety agencies is important to the successful implementation of JUSTIS. A core functionality of JUSTIS is to allow for data sharing from a variety of legacy systems and agency collaboration. The knowledge of the legacy systems allows the implementation team to design strategies for data extraction, inquiry and presentation through JUSTIS. These activities require the analysis of current systems security infrastructure, network infrastructure, user workstations, and legacy applications and the data contained therein. Analysis of the current business processes that are rudimentary attempts to provide similar JUSTIS functionalities are also critical to the JUSTIS implementation team. This avoids reinvention of current processes and lends itself to the expansion of the current system to future phases by taking advantage of current agency relationships. This requires less change management throughout the agencies than would implementations that employ new business processes and the development of new relationships.

- **The JUSTIS Roadmap.** Taking JUSTIS from concept to production requires an evaluation and comparison of the public safety agencies current systems versus the

end solution architecture. Involved in this comparison is the identification of gap areas between the two states and the prioritization of those gap areas. Following the multi-phased implementation strategy these gap areas are prioritized based upon a logical technological progression. By considering the results of closing each gap area, the gap areas are turned into implementation phases. These phases are prioritized based upon the phases' business impact and execution ease providing a roadmap that will lead to the successful implementation of JUSTIS as described in the Blueprint. The first phase and second phases described in the roadmap have been officially defined by the CJCC as statements of work (SOW). These SOWs have been contracted to system developers and are in process. The first phase was the JUSTIS Proof of Concept and was completed and delivered on January 17 2001. The second phase is JUSTIS Phase 2 and is scheduled for completion September 18, 2001.

- **JUSTIS Administrative and Management Structure.** The need for a JUSTIS Administrative and Management Office is critical to the JUSTIS implementation strategy. A multi-phased implementation across various entities requires a centralized and focused management team. The Blueprint defines and proposed structure that will expand as JUSTIS expands and will ultimately be able to perform the following duties:

  - System Operations
  - Help Desk
  - Application Development
  - Application Maintenance
  - Security Management
  - Change Management

It is important to realize that the Blueprint describes the conceptual administrative and management structure. During the implementation of JUSTIS the administrative and management structure will be developed in consideration of not only the conceptual design in the Blueprint but the security management control requirements as described in the document in the JUSTIS Phase 2 deliverable number 1.7, the JUSTIS Security Policy and Procedures document, as well as other relevant external factors.

The JUSTIS Blueprint is a deliverable that was defined in the first phase of implementation of JUSTIS. It is a result of the knowledge gained through analysis of the District of Columbia justice community and has been refined and validated through the implementation of the JUSTIS Proof Of Concept and Phase 2. It was compiled and written in consideration of CJCC requirements and constraints.

This document was first delivered in draft form on August 31, 2000. After the implementation of the JUSTIS POC, the Blueprint was updated to include the most relevant information. The Blueprint will remain a "living" document and will be updated periodically throughout the implementation of JUSTIS. This current draft represents the final update of the Blueprint for Phase 2. Its scheduled delivery date is September 14, 2001. Items that have been either updated or added to the Blueprint since its last delivery are:

- **References to Phase 2 Deliverables** – In order to reduce the size of the Blueprint and to ease the reading, references to the JUSTIS Phase 2 deliverables were added where necessary.
- **More Precise Functionality Description** – The past Blueprints have included general descriptions of the functionality that can be enabled with the implementation of JUSTIS. As the system nears its final phase more accurate descriptions of the functionalities to be implemented are developed. This provides the reader with a more detailed and system specific description of the proposed JUSTIS functionality.
- **Current Systems Summary** – The Current Systems Summary has been modified to include a more up to date Phase 2 infrastructure.

Roadmap – To accurately reflect the scope of work that was included as a part of Phase 2, the roadmap that was outlined in the Blueprint submitted on June 5, 2001 has been modified accordingly. Also, this document incorporates tasks that are to be delivered in Phase 3. The roadmap included in the Blueprint submitted on June 5, 2001 outlined a proposed JUSTIS management and administrative structure and a proposed phased implementation. External factors have modified the deployment of both of these propositions.

7. Glossary

10Base-T – One of several adaptations of the Ethernet (IEEE 802.3) standard for Local Area Networks (LANs). The 10Base-T standard (also called Twisted Pair Ethernet) uses a twisted-pair cable with maximum lengths of 100 meters.

100Base-T – A relatively new networking standard that supports data transfer rates up to 100 Mbps. 100BASE-T (IEEE 802.3u) is based on the older Ethernet standard. Because it is 10 times faster than Ethernet, it is often referred to as Fast Ethernet.

Access Control List (ACL) – A list of access control entries (ACEs), which contain information about a trustee, such as a user, group of users, or program.

ActiveX – A loosely defined set of technologies developed by Microsoft. An outgrowth of two other Microsoft technologies called OLE (Object Linking and Embedding) and COM (Component Object Model).

API – See “Application Programming Interface”.

Applet – A program designed to be executed from within another application. Unlike an application, applets cannot be executed directly from the operating system.

Application Programming Interface (API) – a set of routines, protocols, and tools for building software applications.

Asynchronous Transfer Mode (ATM) – A network technology based on transferring data in cells or packets of a fixed size.

ATM – See “Asynchronous Transfer Mode”.

Backbone – Network technology used to tie together multiple networks on an enterprise network.

Blue Pages – X.500 service that provides subject-matter listings of organizational programs and activities related to the organization such as the government blue pages.

BOP – Federal Bureau of Prisons

Certificate – See Digital Certificate.

Certificate Authority – A Certificate Authority (CA) issues, verifies, and revokes certificates. The Certificate Authority’s digital signature attests to the binding of the individual’s identity and his public key.

Certificate Revocation List – A certificate revocation list is a list of digital certificates revoked before their scheduled expiration date.

CGI – See “Common Gateway Interface”.

Clear Text – Information transmitted over a network in its original, unencrypted state.

Common Gateway Interface (CGI) – A specification for transferring information between a World Wide Web server and a CGI program. A CGI program is any program designed to accept and return data that conforms to the CGI specification. The program could be written in any programming language, including C, Perl, or Visual Basic.

CSOSA – Court Services and Offender Supervision Agency

DCDC – District of Columbia Department of Corrections

DCSC – Superior Court for the District of Columbia

Digital Certificate – A digital certificate is a non-forgeable, tamper-proof electronic document that attests to the binding of an individual's identity with his or her public key. The information contained in the certificate is verified and sealed with the digital signature of a trusted third party, known as a Certificate Authority (CA). The CA will include in the certificate a range of dates within which it is valid.

Digital Signature – A digital signature is a portion of a message encrypted with a user's private key. The recipient knows that this message and its digital signature could have come only from the owner of the private key corresponding to the public key used to decrypt. Digital signatures not only verify the identity of the signer of messages, but also ensure that the messages have not been changed since their signing.

DHCP – See "Dynamic Host Configuration Protocol.

DMV – District of Columbia Department of Motor Vehicles

Dynamic Host Configuration Protocol (DHCP) – A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

EC/EDI – Electronic Commerce (EC) – applications such as Electronic Data Interchange (EDI) for commerce between business partners (e.g., banks, suppliers, manufacturers).

Encryption/Decryption – Encryption is the scrambling of a message into an unreadable form. Decryption is the reverse: an encrypted message is made readable. A key pair controls both encryption and decryption. If either key encrypts a message or file, only the other key in that pair can decrypt it. For example, if someone encrypts a message or file with an individual's public key, only that individual's private key can decrypt it. This assures message confidentiality. A manageable way to deploy encryption in a large environment is with the use of public key cryptography.

Ethernet – A local-area network (LAN) protocol that uses a bus topology and supports data transfer rates of 10 Mbps.

Extensible Markup Language (XML) – This new standard being developed by W3C is a simplified but strict subset of SGML that has features of validation, structure, and

extensibility. XML is a standardized text format designed specifically for transmitting structured data to web applications.

FDDI – See “Fiber Distributed Data Interface”.

Fiber Distributed Data Interface (FDDI) – A set of protocols for sending digital data over fiber optic cable. Generally used for WAN backbone. Supports data rates of up to 100 Mbps.

File Transfer Protocol (FTP) – A mechanism for transferring files between host computers over TCP/IP. FTP includes host-independent sub-commands for connecting and logging on to remote hosts; uploading and downloading files; listing directory contents; and changing the current working directory.

Firewall – A hardware/software device that restricts access between more than one network. A firewall is generally configured to block all externally initiated access, and to run any permitted internally initiated access via ‘proxy’ agents so that the internal computing device is never communicating directly with an external computing device.

Frame Relay – A packet-switching protocol for connecting devices on a Wide Area Network. Frame Relay networks support data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds

FTP – See “File Transfer Protocol”.

Green Pages – X.500 service that provides browsing and querying of electronic information in documents and catalogs, such as documents statistics, photographs, multimedia records, and publications.

HTML – See “Hypertext Markup Language”.

HTTP – See “Hypertext Transport Protocol”.

Hypertext Markup Language (HTML) – The document encoding standard used for web pages. HTML supports embedded graphics, programs, and links to other objects such as web sites, documents, points within documents, images, and files that will automatically launch other desktop applications.

Hypertext Transport Protocol (HTTP) – The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IETF – See “Internet Engineering Task Force”.

IMAP – See “Internet Messaging Access Protocol”.

International Organization for Standardization (ISO) – ISO is an international organization composed of national standards bodies from over 75 countries, including ANSI (American National Standards Institute).

Internet Engineering Task Force (IETF) – The main standards organization for the Internet.

IPsec – A security protocol in the network layer being developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality.

Internet Messaging Access Protocol (IMAP) – A protocol for retrieving email messages.

Internet Service Provider (ISP) – An organization that provides a connection to the Internet.

Intranet – A network based on TCP/IP (Internet) protocols, but belonging to an organization and accessible only by the organization's members, employees, or other authorized users.

Inter-network Packet Exchange (IPX) – A networking protocol used by the Novell NetWare operating systems. IPX is a datagram protocol used for connectionless communications.

International Telecommunications Union (ITU) – An intergovernmental organization established by the United Nations to develop international standards governing telecommunications.

IPX – See “Inter-network Packet Exchange”.

ISO – See “International Organization for Standardization”.

ISP – See “Internet Service Provider”.

ITAC – Criminal Justice Coordinating Council Information Technology Advisory Committee

ITLO – Criminal Justice Coordinating Council Information Technology Liaison Officer.

ITU – See “International Telecommunications Union”.

Java– A high-level programming language designed to be platform-independent. Java programs can be downloaded to a client as part of an HTML document and executed on that client.

JRSA – Justice Research and Statistics Association.

kbps – Kilobits per second. Speed of data transmission in multiples of 1,024 bits (~128 characters) per second.

KPMG CONSULTING, INC. – KPMG Consulting, Inc.

LAN – See “Local Area Network”.

Legacy system – Generally used to refer to working applications and platforms that do not employ consensus state-of-the-art technology.

Local Area Network (LAN) – A computer network that spans a relatively small area. A LAN generally serves a single building or floor of a building.

Mailhost – A server that routes incoming as well as outgoing email. Mail software (e.g., cc:Mail, MS Exchange) packages can store messages to be accessed by users or route mail to other mailhosts.

Management Information Base (MIB) – A database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized MIB formats that allows any SNMP and RMON tools to monitor any device defined by a MIB.

Mbps – Megabits per second. Speed of data transmission in multiples of 1,048,576 bits (~131,072 characters) per second.

Meta-data or Meta-information – Data about data. Meta-data describes how and when and by whom a particular set of data was collected, and how the data is formatted.

Meta tag – An HTML tag that refers to meta-information, rather than to document text.

MIB – See “Management Information Base”.

MPD – Metropolitan Police Department.

Network News Transfer Protocol (NNTP) – Industry-standard method used by News group servers to receive downloads from an ISP; store the data for a predetermined amount of time, and distribute it to users upon request. The data consists of bulletin-board articles contributed by the Internet community.

NNTP – See “Network News Transfer Protocol”.

OCC – Office of Corporation Counsel.

OLAP – See “On-line analytical processing”.

On-line analytical processing (OLAP) – A category of software tools that provides analysis of data stored in a database. OLAP tools enable users to analyze different dimensions of multidimensional data.

PDF – See “Portable Document Format”.

PDS – Public Defender Service.

Portable Document Format (PDF) – A file format developed by Adobe Systems. Enables viewing of documents on screen as they would be printed.

Point-to-point protocol (PPP) – A protocol that allows a computer to access an Intranet or the Internet via a voice-grade telecommunications line and a modem.

POP3 – See “Post Office Protocol”.

Post Office Protocol (POP3) – A protocol used to retrieve email from a mail server.

PPP – See “Point-to-point Protocol”.

Private key – see Public key cryptography.

PSA – Pretrial Services Agency.

PSWG – Criminal Justice Coordinating Council Privacy and Security Working Group.

Public key – see Public key cryptography.

Public key cryptography – In a system that uses public key cryptography, each user is assigned two unique mathematically-related keys: a public key and a private key. The public key is published; the private key is kept secret, accessible only to the owner. Each key can read messages encrypted with the other key.

Push technology – Enables Internet based service delivery initiated by the information provider, rather than by the information requester.

RAS – See “Remote Access Server”.

RDBMS – See “Relational Database Management System”.

Relational Database Management System (RDBMS) – A collection of programs that enables you to store, modify, and extract information from a database.

Remote Access Server (RAS) – A computer or device that provides network access to users not directly connected to that network. Users generally access a RAS via dial-in modem or ISDN adapter.

Remote Monitoring (RMON) – A network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage.

RMON – See “Remote Monitoring”.

Router – A router is a hardware device that directs data flow between networks. The router’s software determines the best path to the destination computer from the client computer.

S/MIME – See “Secure Multipurpose Internet Mail Extension”.

Secure Multipurpose Internet Mail Extension (S/MIME) – A new version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology.

Search Engine – Software that reads documents and builds indices to collections of documents. This allows the user to search the index for key information, as well as document text.

Serial-line Internet protocol (SLIP) – A protocol that allows a computer to access an Intranet or the Internet via a voice-grade telecommunications line and a modem. SLIP is gradually being replaced by PPP.

SGML – See “Standard Generalized Markup Language”.

SLIP – See “Serial-line Internet protocol”.

SNA – See “Systems Network Architecture”.

SMTP – See “Simple Mail Transport Protocol”.

SNMP – See “Simple Network Management Protocol”.

Systems Network Architecture (SNA) – A set of network protocols developed by IBM to inter-connect mainframe computers.

Simple Network Management Protocol (SNMP) – A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units, to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

Simple Mail Transport Protocol (SMTP) – A protocol for sending email messages between mail servers. SMTP is also used to send messages from a mail client to a mail server.

Standard Generalized Markup Language (SGML) – a system for organizing and tagging elements of a document.

T1 – A dedicated telecommunications connection supporting data rates of 1.544Mbits per second. A T-1 line actually consists of 24 individual channels, each of which supports 64Kbits per second.

T3 – A dedicated telecommunications connection supporting data rates of about 45Mbits per second. A T-3 line actually consists of 672 individual channels, each of which supports 64Kbits per second.

TCP/IP – See “Transmission Control Protocol over Internet Protocol”.

Token Ring – A network that connects computers serially, (computer-to-computer) to form a loop, rather than via a hub, such as Ethernet.

Transaction Process Monitor (TP Monitor) – TP Monitor ensures that a transaction processes to completion and ensures that proper actions are taken if it fails to complete successfully.

Transmission Control Protocol over Internet Protocol (TCP/IP) – The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

TWG – Criminal Justice Coordinating Council Technical Working Group

Uniform Resource Locator (URL) – The standard naming convention used to identify a presence on the world wide web. This location can be a server (www.location.com); a directory on a server (www.location.com/directory); a file on a server (www.location.com/directory/page.html); or a point on a file (www.location.com/page.html#refpoint). The location is preceded by the protocol used to access the location—e.g., http:// (for html documents) or ftp:// (for file transfers).

URL – See “Uniform Resource Locator”.

USAO – United States Attorney’s Office

USPC – United States Parole Commission

Virtual Private Network (VPN) – A network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

W3C – See “World Wide Web Consortium”.

WAN – See “Wide Area Network”.

Web – See “World Wide Web”. When capitalized, “Web” typically refers to the World Wide Web on the Internet; lower-case “web” usually refers to the technology, regardless of whether it is deployed on the Internet or on a private Intranet.

Web Browser – A software application used to access information on a web-based network. A browser presents HTML-formatted documents, and it generally supports other protocols such as FTP.

Web Site – A single Web/Internet or private web/Intranet location (generally a web server or a directory on a web server).

White Pages – Basic “lookup” service for X.500 directories that presents personnel specific information such as telephone numbers, office locations, physical mailing addresses, and other personal and organizational attributes.

Wide Area Network (WAN) – A computer network that spans a relatively large geographical area. Typically, WAN consists of two or more local-area networks (LANs).

World Wide Web (WWW) – A system of Internet servers that support specially formatted documents. The documents are formatted in a language called HTML that supports links to other documents, as well as graphics, audio, and video files.

World Wide Web Consortium (W3C) – Organization of representatives from companies around the world that develops open standards used by the world wide web, such as HTML.

X.500 – An ISO and ITU standard that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. X.500 supports X.400 systems.

X.509 – X.509, or ISO/IEO 9594-8, is widely recognized as the leading network and communications security architecture standard specification. Any application or device can use the standardized security and authentication services of X.509. The authentication-framework specification within X.509 addresses the handling of public keys via certificates and certificate revocation lists.

XML – See “Extensible Markup Language”.

YSA – District of Columbia Department of Human Services Youth Services Administration

Yellow Pages – X.500 service that presents detailed information on products and services to facilitate organizational procurement activities.